





# **Values and Freedoms in Modern Information Law and Ethics**

Values and Freedoms in Modern Information Law and Ethics  
ISBN 978-960-272-979-3



ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ

Μαυρομικάλη 23, 106 80 Αθήνα  
Τηλ.: 210 3678 800 • Fax: 210 3678 819  
<http://www.nb.org> • e-mail: [info@nb.org](mailto:info@nb.org)

Αθήνα: Μαυρομικάλη 2, 106 79 • Τηλ.: 210 3607 521  
Πειραιάς: Φίλωνος 107-109, 185 36 • Τηλ: 210 4184 212  
Πάτρα: Κανάρη 28-30, 262 22 • Τηλ.: 2610 361 600  
Θεσ/νίκη: Φράγκων 1, 546 26 • Τηλ.: 2310 532 134

Σύμφωνα με το Ν. 2121/93 για την Πνευματική Ιδιοκτησία απαγορεύεται η αναδημοσίευση και γενικά η αναπαραγωγή του παρόντος έργου, η αποθήκευσή του σε βάση δεδομένων, η αναμετάδοσή του σε ηλεκτρονική ή οποιαδήποτε άλλη μορφή και η φωτοανατύπωσή του με οποιονδήποτε τρόπο, χωρίς γραπτή άδεια του εκδότη.

#### ΔΗΛΩΣΗ ΕΚΔΟΤΙΚΟΥ ΟΙΚΟΥ

Το περιεχόμενο του παρόντος έργου έχει τύχει επιμελούς και αναλυτικής επιστημονικής επεξεργασίας. Ο εκδοτικός οίκος και οι συντάκτες δεν παρέχουν διά του παρόντος νομικές συμβουλές ή παρεμφερείς συμβουλευτικές υπηρεσίες, ουδεμία δε ευθύνη φέρουν για τυχόν ζημία τρίτου λόγω ενέργειας ή παράλειψης που βασίστηκε εν όλω ή εν μέρει στο περιεχόμενο του παρόντος έργου.

Art Director: Θεόδωρος Μαστρογιάννης  
Υπεύθυνος Παραγωγής: Ανδρέας Μενούνος  
Φωτοστοιχειοθεσία: Αριστέα Διακουμπούλου  
Παραγωγή: NB Production AM210512M23

#### ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ GROUP

23, Mavromichali Str., 106 80 Athens Greece  
Tel.: +30 210 3678 800 • Fax: +30 210 3678 819  
<http://www.nb.org> • e-mail: [info@nb.org](mailto:info@nb.org)



member of Europe's top  
universities



Committed to excellence

© 2012, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ ΑΕΒΕ

Proceedings of the 4<sup>th</sup> International Conference  
on Information Law and Ethics

Edited by Bottis Maria, Alexandropoulou Eugenia,  
Ioannis Iglezakis

# Values and Freedoms in Modern Information Law and Ethics

- Information Law
- Privacy and Data Protection
- Freedom of Information
  - Surveillance
- Social Networks and the law
- Philosophy of information
  - Intellectual property

Forward: Herman Tavani, *Professor*



NOMIKI BIBLIOTHIKI



## Contents

A message from Professor Herman Tavani, INSEIT President .....	1
A note on the International Conference on Information Law .....	3
The individuals' fragmented political autonomy: surveillance of public spaces, anonymity and the myth of "public security" .....	7
<i>Christina Akrivopoulou</i>	
Social Network Sites (SNS): a harmless remarkable technological phenomenon or a harmful backdoor with long-term unpredictable consequences? .....	17
<i>Konstantina Alexopoulou</i>	
E-ID card & data protection: a path for good governance – a field of controversy .....	41
<i>Athina Antoniou &amp; Lilian Mitrou</i>	
The European Commission's policy on the harmonization of protection of the moral rights of authors and performers in the European Union .....	51
<i>Theodore Asprogerakas – Grivas</i>	
The threat to consumers' privacy: digital management systems of protection of privacy and personal data .....	59
<i>Victoria Banti-Markouti</i>	
The scope of 'protective' European private international law rules in electronic consumer contracts: the Court of Justice of the European Union tackles the problem in the cases Pammer and Alpenhof .....	70
<i>Bertel De Groote</i>	
Mass digitisation and the moral right of integrity .....	90
<i>Maurizio Borghi</i>	
From theory to practice: autonomy, privacy and the ethical assessment of ICT .....	106
<i>William Bülow &amp; Misse Wester</i>	

Evolution of data protection starting from the French experiment, in a context of vicinity: solutions and new questions - prospects .....	113
<i>Georges Chatillon</i>	
The criminalization of hacking tools as a reasonable measure of protection regarding attacks against information systems and computer data .....	123
<i>Konstantinos Chatziioannou</i>	
Private power and new media: the case of the corporate suppression of WikiLeaks and its implications for the exercise of fundamental rights on the Internet .....	136
<i>Angela Daly</i>	
Rethinking about freedom and ethics in the era of networks: new trends in journalism ethics.....	156
<i>Elsa Deliyanni</i>	
IMEDIATV: Open and interactive access for live performances and installation art.....	169
<i>Ioannis Deliyannis, Ioannis Karydis &amp; Dimitra Karydi</i>	
Recent developments of the Bulgarian trademark legislation and practice.....	186
<i>Jivko Draganov</i>	
Can the EU's data protection rules survive data transfers to third states? .....	202
<i>Els De Busser</i>	
E-government adoption in the EU: theoretical and methodological challenges in the study of the digital divide .....	227
<i>Georgia Foteinou</i>	
Libraries and the role of copyright exceptions and limitations in the contemporary academic environment.....	246
<i>Anna Fragkou &amp; Vassiliki Strakantouna</i>	
RIPE NCC - Internet governance and registration of IP addresses .....	268
<i>Athina Fragkouli</i>	



The EU Data Protection Directive revised: new challenges and perspectives .....	286
<i>Maria Giannakaki</i>	
A Web-based application for the registration of intellectual property .....	306
<i>Andreas Giannakouloupoulos</i>	
Digital disposition of a work: from technical protection measures to creative commons .....	321
<i>Alexandra Giannopoulou</i>	
The old ethical problems in the new information society in Russia .....	332
<i>Vitaly Gorokhov</i>	
Regulation models addressing data protection issues in the EU concerning RFID technology .....	350
<i>Ioannis Iglezakis</i>	
Video games and the law .....	359
<i>Philippe Jougoux</i>	
Copyright holders and peer-to-peer network users: an uncompromised relationship? .....	370
<i>Archontoula Kapsi</i>	
Surveillance in the workplace: new technologies, new challenges, new solutions? .....	389
<i>Eleni Karakolidou &amp; Lilian Mitrou</i>	
Consent for data processing in e-commerce transactions: UK empirical evidence .....	406
<i>Stavroula Karapapa &amp; Indranath Gupta</i>	
Personal data protection in the era of cloud computing new challenges for European regulators .....	431
<i>Panagiotis Kitsos &amp; Paraskevi Pappa</i>	
Patenting human genes in Europe: is it possible to set an ethical minimum based on common values? .....	444
<i>Leandros Lefakis</i>	

Rejecting the works of Dan Flavin and Bill Viola: revisiting the boundaries of copyright protection for post-modern art.....	458
<i>Marina Markellou</i>	
Audiovisual works as intellectual property .....	466
<i>Maria Markova</i>	
Freedom of the press in the eyes of Nigerian Law.....	477
<i>Maureen Ifeyinwa Nwanolue &amp; Edith Chinelo Ude-Akpe</i>	
Profiling and manipulating human behaviour: a core contemporary privacy concern.....	487
<i>Alan McKenna</i>	
The struggle over privacy, security, cyber-crimes and the civil rights in the Brazilian law – a historical overview .....	508
<i>Rubens Menezes de Souza</i>	
Passage of freedom of information bill in Nigeria: the unending journey .....	533
<i>Mercy Ifeyinwa Anyaegbu &amp; Rose Obiozor-Ekeze</i>	
HADOPI 1 & 2: analysis and evaluation .....	555
<i>Eleni Metaxa</i>	
Social networking and the employment relationship .....	562
<i>Stathis Mihos</i>	
Personal financial data in danger: the case of the new smart tax-card in Greece .....	575
<i>Milossi Maria &amp; Alexandropoulou Evgenia</i>	
E-privacy in practice.....	581
<i>Misic Klemen</i>	
Public domain vigor in copyright based on John Locke.....	588
<i>Marinos Papadopoulos &amp; Alexandra Kaponi</i>	
Online gambling and EU Law .....	623
<i>Thomas Papadopoulos</i>	

ACTA and copyright in EU: a love or hate relationship? .....	638
<i>Maria Daphne Papadopoulou</i>	
The idea of legal convergence and electronic law .....	679
<i>Antonios Platsas</i>	
European public sphere and digital political communication: Facebook as a medium of political expression and participation .....	689
<i>Helen Rethimiotaki</i>	
On uploading and downloading copyrighted works: the potential legality of the users' interest in engaging in such acts - the case of EU and US paradigm.....	709
<i>Vasiliki Samartzi</i>	
YouTube, YouRisk, YouProtect - copyright issues.....	728
<i>Maria Sinanidou</i>	
From online diaries to online 'unmonitored' media?.....	755
<i>Evgenia Smyrnaki</i>	
Self-determination and information privacy: a plotinian virtue ethics approach.....	779
<i>Giannis Stamatellos</i>	
Towards an updated EU Enforcement Directive? Selected topics and problems .....	792
<i>Irini Stamatoudi</i>	
Evaluating the quality of e-democracy processes: an empirical study in the Greek context .....	807
<i>Stiakakis Emmanouil &amp; Tongaridou Konstantina</i>	
The principle of technological neutrality in European copyright law: myth or reality?.....	826
<i>Tatiana – Eleni Synodinou</i>	
Regulation and self-regulation of online activity Blogs and electronic social media.....	842
<i>Spiros Tassis</i>	
Beyond the boundaries of open, closed and pirate archives: lessons from a hybrid approach.....	857
<i>Prodromos Tsiavos &amp; Petros Stefaneas</i>	

Transposing the Data Retention Directive in Greece: lessons from Karlsruhe.....	883
---	-----

*Anna Tsiftoglou & Spyridon Flogaitis*

Enforceability of free/open source software licensing terms: a critical review of the global case - law .....	898
---	-----

*Thanos Tsingos*

Law and ethics in the modern EU ‘surveillance society’: are data protection principles ‘dead’ in the area of freedom, security and justice? The case of VIS and EURODAC information systems .....	941
---	-----

*Maria Tzanou*

Inconsistencies in the regulation of anti-circumvention in the EU .....	961
---	-----

*Petroula Vantsiouri*

“All that is solid melts into air”: the history of copyright as a form of industrial regulation and its disorientation in the age of information .....	976
--	-----

*Nikolaos Volanis*

Mobile devices, virtual presence, and surveillance: questions concerning epistemology and some new challenges for privacy and data protection.....	997
--	-----

*Karsten Weber*

Information Technology, millennials and privacy: can they blend or will they collide? .....	1007
---	------

*Aharon Yadin*

Technology beats the law? .....	1024
---------------------------------	------

*Georgios Yannopoulos*

## **YOUNG SCHOLARS’ FORUM**

The legal framework of personal data e-processing in the digital environment in Greece .....	1035
--	------

*Konstantina Arkouli*

The Budapest’s Convention as a guarantee limit against cybercrime.....	1051
--	------

*Eleni Chrysopoulou*

Ethical implications concerning the access to and use of information and the technologies.....	1072
<i>Antonio Cobos Flores</i>	
Online copyright infringement provisions within UK's Digital Economy Act, 2010 - Are Internet Service Providers legally responsible for their subscribers?.....	1081
<i>Eben Duah</i>	
When Personalization Becomes Too Personal.....	1102
<i>Christina Gkarnara</i>	
Knowledge as a public or private good? A new twist to an old tale A comparative human rights analysis of the protection of knowledge creation and diffusion.....	1116
<i>Katarzyna Gracz</i>	
Institutional open access repositories in college education: a proposal for their role in open educational resources in Greece .....	1139
<i>Nikos Koutras, Elisa Makridou &amp; Iliana Araka</i>	
Building an inclusive information society at the local level in Estonia .....	1160
<i>Liia Laanes</i>	
Recent developments in the transnational information exchange between law enforcement authorities in the EU: The introduction and implementation of the principle of availability.....	1175
<i>Konstantia-Christine Lachana</i>	
I (do not) consent to behavioural advertising .....	1200
<i>Evangelia Mesaikou</i>	
RFID in the supply chain and the privacy concerns.....	1212
<i>Nikita Maria</i>	
Ethics in scholarly publishing: the journal editor' s role .....	1234
<i>Anna-Maria Olenoglou</i>	
State-based internet censorship: direct or delegated practices and their effects on the free flow and future of the internet .....	1245
<i>Kyriaki Pavlidou</i>	

Internet child pornography and problems in relation to its criminalization .....	1274
<i>Vaiani-Vagia Polyzoidou</i>	
“Illegally obtained evidence and their use in civil procedure” .....	1286
<i>Ioannis Revolidis</i>	
Advergaming: A lawyer’s take .....	1300
<i>Veljko Smiljanić</i>	
The Google library project and its international dimensions.....	1318
<i>Antigoni Trachaliou</i>	
Electronic government: its course in United States, European Union & Greece.....	1340
<i>Aikaterini Yiannoukakou</i>	

## **A message from Professor Herman Tavani, INSEIT President**

On behalf of the International Society for Ethics and Information Technology (INSEIT), I am delighted to congratulate Associate Professor Tzeni Alexandropoulou, Assistant Maria Bottis and Assistant Professor Ioannis Iglezakis who have put together yet another highly successful conference in the ICIL series: ICIL 2011, in Thessaloniki, Greece. INSEIT has been a proud sponsor of the ICIL 2009, 2010, and 2011 Conferences, and is pleased to serve as a sponsor for the ISIL 2012 Conference, which will be held in Corfu, Greece in late June 2012. I personally have enjoyed working closely with Assistant Professor Bottis who, I believe, has also done an outstanding job of forming a strong professional connection between the ICIL conference series and INSEIT, and between that conference series and the CEPE (Computer Ethics: Philosophical Enquiry) series, which is also sponsored by INSEIT. ICIL has now become a premier international conference and INSEIT welcomes the opportunity to sponsor more ICIL conferences in the future.

***Herman T. Tavani***

*INSEIT President*

*November 2011*





## **A note on the International Conference on Information Law**

The International Conference on Information Law (ICIL) is an international event organized by the Department of Archive and Library Science of the Ionian University, as the main organizer and it started as an activity of the Postgraduate Program of the Department of Archives and Library Science in Corfu, titled “Science of Information”, in 2008, in Corfu.

The first conference in Corfu, in 2008, was titled “The changing facets of Information in Information Law”. In 2009, the conference was held jointly with an international event, the 8th International Conference of Computer Ethics: Philosophical Enquiry (CEPE), a conference the Department of Archive and Library Sciences co-organized with the Department of Informatics of the Ionian University.

CEPE conferences are sponsored by INSEIT, the International Society for Ethics and Information Technology. INSEIT gladly agreed to also sponsor the ICIL series, starting with the year of 2009, with “A World for Information Law”, in Corfu. In 2010, with “An information Law for the 21st Century”, in Corfu, ICIL accepted more than 35 papers and presentations; the keynote speakers were President Commissioner Oscar Guerra Mauricio Ford, from Mexico, head of the Institute for Access to Information for the Federal District, Mexico, Professor emeritus Lambros Kotsiris from the Thessaloniki Law School, an esteemed member of the Hellenic Academy and Dr. Konstantinos Karachalios, Analyst, from the European Patent Office. This was the first year a forum for young scholars was added to ICIL, the Young Scholars’ Forum.

The thematic area covered in ICIL is wide-very wide, indeed. It covers every legal aspect of dealing with information, for example every legal aspect of dealing with the production, transfer, access, ownership, use and management of information; it also covers privacy, data protection, intellectual property, freedom of information and the rules on the use of new information technologies (IT law). Information law, as it also includes Information Technology Law, is of course a very wide field; it is obvious in the very diverse topics of our papers presentation an example of how wide this can actually be. Coming to information ethics, and being very grateful to Professor Rafael Capurro who came to Corfu in 2009 to teach us about information ethics, it is evident that information law and information ethics constitute an inseparable unit of an academic domain. Researching information law and not information ethics, at least as “basics”, is wrong; it deducts from the discussion the philosophical foundation without which the strictly legal

‘conversation’ turns out almost unimportant. Because law may give us tools to resolve some questions in practice, the method to adjudicate a dispute and to give an award to this or the other party-yes, this is true, but ethics is the reason you ever reach to articulate the question itself. This said, ICIL covers both information law and ethics and actively seeks academics and scholars in both connected fields.

And this brings us to this 4th international conference (ICIL) of 2011, ‘Values and Freedoms in Information Law and Ethics’, which took place in Thessaloniki, at the University of Macedonia, which was the main financial sponsor of the Conference. ICIL changed venue, wishing to attract more people who would come easier to a big city like Thessaloniki. It was co-organized by the University of Macedonia (co-chair, Assoc. Professor Eugenia Alexandropoulou) and the Aristotle University of Thessaloniki (co-chair, Ass. Professor Ioannis Iglezakis).

ICIL 2011 was morally sponsored, except by INSEIT, also by the Institute of Legal Informatics of Germany (thank you Professor Forgo, for also sending us a fan of ICIL, joining for a third time, Marcelo Corrales-IRI also sponsored ISIL 2010), by the Italian NEXA Center for Internet and Society and by the International Center for Information Ethics (ICIE) (thank you Professor Rafael Capurro, for sending us Professor Karsten Weber, as an ICIE representative). Let us express our gratitude for this invaluable moral support. And, of course, our gratitude must be also expressed to our financial sponsors, the University of Macedonia, the Ionian University, the Aristotle University of Thessaloniki, the publisher Nomiki Vivliothiki (thank you so much Lila Karatza, for always being there for us) and the Thessaloniki Bar Association.

We also need to thank, from our hearts, Dr. Andreas Giannakouloupoulos, Lecturer, Ionian University and Roubini Economou who had the responsibility for the ICIL site (the conference would not have happened without their help). We thank Maroula Selemenou, for her help in the work for this volume. We thank Maria Mavrona, Rania Konsta, Gianna Siameti, Nikos Anastasiou, Katerina Tzali and Thanos Dampas from the Ionian University. We thank Roxana Theodorou, for her excellent work on the ICIL program. We thank Dionyssis Kourtesis for the ICIL 2011 poster design. We thank all the rest members of the executive organizing committee of the conference from Macedonia, and especially, Dr. Panos Kitsos and the PhD candidates (IT Law) of the University of Macedonia, Maria Milossi, Katerina Yannoukakou, Efi Moschidou, Elina Chryssopoulou and Maria Nikita for their constant help and support in the Conference and in the work for the present proceedings, as well as the team of postgraduate and undergraduate students of the University of Macedonia for their assistance. We thank Aristeia Diakoumopoulou, from Nomiki Bibliothiki for her excellent work in preparation of this volume and for her unbelievable patience. At last, but not least, we need to thank Mariet Vaina, head of public relations of the University of Macedonia for her professional services. Thank you all.

Participation in ICIL 2011 greatly surpassed expectations. We had more than 130 speakers, from all over the world. The 2010 volume of proceedings exceeded 700 pages. The ICIL 2011 book of proceedings comes up to more than 1.300 pages and this is, to us, an important contribution to the evolution of information law scholarship and development.

**Maria Bottis**

Assistant Professor, Ionian University

**Eugenia Alexandropoulou**

Associate Professor, University of Macedonia

**Ioannis Iglezakis**

Assistant Professor, Aristotle University of Thessaloniki



# **The individuals' fragmented political autonomy: surveillance of public spaces, anonymity and the myth of "public security"**

---

---

**Christina Akrivopoulou**

---

---

## **1. A global and Greek overview of the 'Public Camera Surveillance' phenomenon**

The famous Orwell's phrase could adequately describe the state of affairs as far as the expansion of public surveillance in all over the world is concerned: 'Big Brother is watching you'<sup>1</sup>. For many this phrase provides the comfort of public safety in an unsafe, especially after the September 11<sup>th</sup>, era. Yet, for others it marks the transition to a society that threatens fundamental rights and freedoms. The reality is the following. As international statistics inform us, in the USA since 2003 the CCTV systems (Closed Circuit Television) have expanded from 2.000.000 to 30.000.000. It is reported that nowadays 2.000.000-3.000.000 CCTV systems are introduced each year in order to serve commercial, government or research purposes.<sup>2</sup> After the September 11<sup>th</sup> in the area of Manhattan more than 10.000 functioning CCTV systems are functioning, especially in the famous 'Ring of Steel', an area that encircles Wall Street and the World Trade Center. The most sophisticated system of 'Public Camera Surveillance'<sup>3</sup> can be found in Washington D.C. where the CCTV technology based on 'satellite optics' provides with the most accurate system of surveillance globally. As far as pedestrians, workers and everyday shoppers are concerned, the use of such systems approximately catches them at 200-300 instances of their everyday life.<sup>4</sup> In the UK only there are 800 programs of public surveillance in action and approximately 2.000.000-3.000.000 CCTV systems functioning (fortunately only 200.000-400.000 of them in public areas). The Principedom of Monaco is a 100% surveilled area, whereas Australia is using extensively the CCTV systems with 40.000 func-

---

1. See G. Orwell, 1984, Penguin, New York 1948.

2. See M. McCahill/C. Norris, On the threshold to Urban Panopticon: Analyzing the employment of CCTV in european cities and assessing its social and political impacts, *Working Paper No 6*, Centre for Criminology and Criminal Justice, University of Hull, UK 2002.

3. Abbreviation used instead of the term CCTV.

4. See D. Aaronovitch, The strange case of the Surveillance Cameras, *The Sunday Times*, March 3, 2009.

tioning in Melburn. Japan and China also use CCTV systems extensively. Since the Olympic Games 260.000 CCTV systems are functioning in Pei Jin only.

In France, approximately 340.000 CCTV systems are in use, a number augmented after the terrorist attacks in Spain and the UK. In Sweden, the application of hidden CCTV systems is banned. The use of 'Public Camera Surveillance' is issued only for research or public interest purposes and only when the public is adequately informed of its presence according to the 'Public Camera Surveillance Act [56]' of 1998.<sup>5</sup> In Italy, the national Data Protection Authority requires a specific survey on the necessity of 'Public Camera Surveillance' in order to authorize its use. In the Netherlands, 'Public Camera Surveillance' is permitted only if the public is previously informed about the presence of CCTV systems in function. In Switzerland the CCTV systems employed bear the capacity to automatically encrypt the information which the competent authorities can decode, only in cases that criminal actions have taken place. Greece provides with a much lower statistics (a little more than 1000 CCTV systems in function, mainly used in monitoring traffic circulation) as most of the EU countries due to the reluctance and limitations that the national Data Protection Authorities poses.

In Greece, the public and theoretical dialogue concerning public surveillance was initiated by the Parliamentary legislation (Act 3625/2007), which acknowledged the legitimate use of cameras during public demonstrations and manifestations in Greece. The scope of the legislative intervention was to protect public safety, public security and private property against acts of violence that were occurring during such public demonstrations. The legislative intervention followed an 'institutional' conflict between the Attorney of the Court of Cassation and the Council of the Data Protection Authority, which ended in a political crisis and the resignation of all members of the Independent Authority.<sup>6</sup> Subsequently, the relevant legislation is still existing but not enacted. More recently, in the summer of 2009, an amendment of the 'basic' data protection legislation (Law 2472/1997, Art. 8) has enabled the use of over a 1000 CCTV cameras in public spaces and

---

5. Nevertheless, Sweden has introduced a legislative package (known as Fra-lagen) that authorizes the warrantless surveillance of all means of communications (telephone, internet etc). Since now it has faced a strong criticism and may soon be tried in front of the ECtHR as far as the violation of human rights (privacy, dignity, personality and freedom of communication) is concerned. See M. Klamberg, Fra and the ECHR- A Paradigm Shift in Swedish Electronic Surveillance Law, in *Nordic Yearbook of Law and Information Technology*, Fagforlaget, Bergen 2010, pp. 96-134.

6. See H. Anthopoulos, The electronic surveillance of Public Assemblies: Political Privacy & Public Anonymity in Greece, in *Personal Data Privacy and Protection in a Surveillance Era*, (edit. Ch. Akriopoulou/Ath. Psygkas) Information Science Reference, Hersey-New York, 2011, pp. 59-68.

the relevant retention of data for the short period of a week, despite the strong objections of the Greek DPA as far as the protection of privacy and dignity is concerned.<sup>7</sup>

## 2. The lost private/public sphere boundary and the consequences for the political participation

The division between the public and private sphere is introduced in theory in the work of Hannah Arendt.<sup>8</sup> Arendt is presenting in her work the private/public demarcation initially as an absolute one that has gradually blurred due to the parallel construction of a third, intermediate sphere, the social. In this line, the private sphere represents a space connected to the family life and intimacy of the individual, where she can develop freely her sexuality, her ethical views and values. At the same time, the public sphere represents the common place which everyone can share and where everyone can meet, communicate and exchange politically, or held accountable in the political deliberation. The third sphere, the social is the sphere of the economy, of property and professional life, where the subject is acting as an individual and not as a citizen.

This division, extremely useful in theory and jurisprudence in order to define the normative consequences of civil, political and social rights, is actually defied in practice. Therefore, many theorists justly doubt its absolute character, noting that many human practices in the course of history have reshaped from private to public (e.g. the naked body which constituted a symbol of strength and was publicly demonstrated in ancient Greece, while is today protected as the core of human intimacy).<sup>9</sup> Nevertheless, nowadays one could claim that public and private can be represented more as *spatium mixtus* and less as a clear dichotomy. The main reason for such a paradigm shift is the privatization of the public sphere due to the connection of the public space with the notion of property and the transfer of private and intimate life to the public sphere. To this direction, 'Public Camera Surveillance' serves as the rhetoric or the symbol for this transfiguration.

Terrorist attacks taking place in all over the world, with their epicenter the September 11<sup>th</sup>, as well as the augmentation of crime has given rise to the notion of public safety and the protection of community in most of the modern representa-

---

7. See A. Tsiftoglou, Surveillance in Public Spaces as a Means of Protecting Security: Questions of Legitimacy and Policy, in *Personal Data Privacy and Protection in a Surveillance Era*, op. cit. pp. 93-103.

8. See H. Arendt, *The Human Condition (Vita Activa)*, The University of Chicago Press, Chicago 1958.

9. See D. Solove, Conceptualizing Privacy, *California Law Journal*, 2002, pp. 1087-1156.

tive democracies. Those arguments are based in the communitarian perspective that community values, such as public safety, should be prioritized to the protection of civil liberties and political rights. Such argumentation can be additionally reinforced in countries such as Greece, where political participation in some occasions has lead to violence.<sup>10</sup> Nevertheless, this approach apart from its generalizing rhetoric (in most cases it restricts the freedom of the majority based on the actions of a small minority) it is based on the connection of public safety and public space with the notion of *private property*. Thus, the notion of public safety this approach proposes is less a public, common, community value and more the sum of private, individual interests. This is why it is often combined with arguments concerning the need for protecting private property against violent or criminal acts. Along this line, surveillance seems a justified solution, since it is the best provision of protecting private property. In today's society one does not have to build a 'fence' or guard her acquisitions if she can electronically protect them. Yet it should be noted that the public sphere is a place not *owned* but *shared* by all. According to this argument, 'Public Camera Surveillance' is actually functioning as a metaphoric bridge that transfers the private to the public sphere.

The second reason for the privatization of the public sphere lays in the modern culture of our public communication and social exchange which becomes more and more privatized. It is a phenomenon that Richard Sennet has vigorously described as the 'tyranny of intimacy'.<sup>11</sup> Thus, even the public space, public figures and public actions are evaluated in terms of privacy e.g. in many cases the politicians are evaluated not according to their public work but with criteria such as their family relations, sexual choices etc. However, we must concur that the individual is not entering the public sphere naked or devoid of any personal characteristics, even beliefs, which in many occasions become of stake in the public deliberation (e.g. gender or homosexuality), we should nevertheless underline the following. In the traditional private/public division the public sphere is not nowadays the space of the monumental and great political acts since it has transfigured to a sphere of quotidian life, where even the political discourse becomes an everyday routine. The indiscriminate surveillance of common, anonymous everyday people transfers the culture of intimacy into the public sphere.

---

10. We are specifically referring to the Greek December of 2008, when public demonstrations have lead to an unseen for Greece violence in the streets of Athens, Thessaloniki and other Greek cities. It was these events that triggered the adoption of legislative measures of the 'Public Camera Surveillance' of public demonstrations in Greece. See A. Kalyvas, An anomaly? Some reflections on the Greek December of 2008, *Constellations*, 2010, pp. 315-365.

11. See R. Sennet, *The Fall of Public Man*, Alfred A. Knopf, New York, 1976.



### 3. Debating public surveillance: arguments pro and against the use of CCTV technology in public spaces

In theory, there are arguments in favor and against 'Public Camera Surveillance'. The arguments supporting its use underline its importance for public safety, private property and mainly for confronting terrorism and deterring crime. Those supporting the use of 'Public Camera Surveillance' also emphasize that in the near future when the CCTV's will not be operated manually but with the use of motion detection systems, their use will become the most valuable remedy against criminal activity and terror. The main legitimizing line of thought is based on the distinction between the lawful and unlawful citizen according to which the first do not face any threats or risks by the use of their data, since they are not in any way implicated in criminal activities.<sup>12</sup> In this perspective, the protection of community as a whole is hierarchized as more important than the protection of the basic individual rights and freedoms that the 'Public Camera Surveillance' is jeopardizing, namely privacy and dignity.<sup>13</sup> Seen critically the main threat posed by this point of view is its attachment to the use of the symbolic power that any argument based on a community's common values bears, a symbolic power that in some cases can be proved to be misleading.<sup>14</sup>

The arguments against bring forward the high cost of the use of the CCTV systems in comparison with alternative measures, such as specialized police forces, patrols etc. and mainly their low deterring effects. In Australia, the statistics show that one arrest every 160 days is occurring due to 'Public Camera Surveillance'. In Italy, a 28% increase of bank robberies has followed the expansion in the use of CCTV systems.<sup>15</sup> Many theorists observe that cameras are not effective deterrents since in most cases their presence is not stated to the possible offenders and thus their use for preventing crime is minimized. In several cases the taped material is destroyed before it could be used in order to resolve a crime and in others, the possibility of identifying a criminal is jeopardized by the poor

12. See K. Günther, *World Citizens between Freedom and Security, Constellations*, 2005, 379-391.

13. See M. Foucault, *Society Must be Defended. Lectures at the Collège de France, 1975-1976*. (trans. D. Macey), Picador, New York, 2003.

14. See M. Neves, *The symbolic force of human rights, Philosophy & Social Criticism*, 2007, σελ. 411-444.

15. See an analogous argument in the ECtHR case, *K. H. & Marper versus UK*, 4<sup>th</sup> December of 2008. The ECtHR in this famous case has underlined that there are no reliable statistic or survey that can prove beyond doubt a connection between harvesting and processing personal, genetic or other personal data and crime prevention or detention.

quality of the recording, or needs more specific analyses and interpretation.<sup>16</sup> In those cases, objective statistics on their use against crime show that any notable reduction of crime connects with specific kind of criminal activities, namely robberies and thefts (e.g. the example of Newcastle, where a 21% drop in thefts was noticed, one of the highest percentages globally by the use of 'Public Camera Surveillance').

As far as theory and jurisprudence are concerned, it must be noted that a strong criticism derives from the fact that in many cases 'Public Camera Surveillance' tends to generalize for the vast majority acts that concern a much smaller minority. The 'chilling effect' of such kind of surveillance also presents a counter argument. Thus in the famous case *Peck versus UK*,<sup>17</sup> the ECHR strongly underlined the effects of such a surveillance for the autonomy and freedom of the individual as well as the possible risks that could derive even by innocent activities of the individual by the future use of recorded material. Especially in the case of the surveillance of public, political activities such as demonstrations and political manifestations, those risks are significantly augmented, since they could deter the freedom of expressing political ideas and thus, they could deter public, political participation.<sup>18</sup>

In such cases one could object: when someone is moving in the public sphere where everything and everyone is transparent and observable by the others, how she can expect the constitutional protection of privacy, a notion combined with secrecy, confidentiality and freedom in the private sphere? This is the very opinion of the U.S. Supreme Court in the case of *U.S. versus Knotts*<sup>19</sup> when it stated that monitoring cars with an electronic beeper does not violate the individuals' reasonable expectation of privacy.<sup>20</sup> What is here supported is that privacy is not limited by space, public or private and that is as closely connected with our sentiments and thoughts as with our words and our public communication, contact and actions. Such a broad conception of privacy can safeguard the freedom and

---

16. See Ch. Slobogin, «Surveillance and the Constitution», *Wayne Law Review*, 2009, pp. 1105-1130.

17. See the ECtHR case *Peck versus UK*, 1<sup>st</sup> November 2001.

18. See Ch. Slobogin, *Privacy at Risk: The new government surveillance and the Fourth Amendment*, The University of Chicago Press, Chicago, 2007.

19. 460 US 276 (1983).

20. For the notion of 'reasonable expectation of privacy' in the international jurisprudence see the case of the US Supreme Court, *Katz v. US*, 389 US 347 and the analogous ECtHR case *Von Hannover v. Germany*, 24<sup>th</sup> June 2004. Also see, C. Boa, *Privacy outside the Castle: Surveillance Technologies and Reasonable Expectations of Privacy in Canadian Judicial Reasoning*, *Surveillance & Society*, 2007, pp. 329-345.

autonomy of the individual especially in those legal orders where there is no sufficient legislation to regulate the violations of fundamental rights occurring by the use of 'Public Camera Surveillance' (the case in the other side of the Atlantic where such government policies are only restricted by soft law, 'Guides of Conduct' etc.).

#### **4. The scope of protecting public privacy and the right to anonymity**

The central argument of this paper is that a right to public privacy, a right to public anonymity must be deducted from the traditional notion of privacy in order to protect the individual in the public sphere. This right can be used as a guide map for the judiciary in the judicial review of legislation that restricts public autonomy by the use of CCTV systems and in order to weight the proportionality of administrative measures enforcing such legislations. The association between privacy and anonymity is not new. In the American bibliography it has been supported by Allan Westin and Christofer Slobogin. According to Westin anonymity is a 'state of privacy' that 'occurs when the individual is in public places or performing public acts but still seeks and finds, freedom from identification and surveillance'.<sup>21</sup> According to Slobogin in this state an individual is able 'to merge into the situational-landscape'.<sup>22</sup> The value of protecting the right to anonymity is that thus the individual can enjoy her autonomy in the public sphere without restraining or abstain from actions that can cause her any political or social discrimination, stigmatization, social humiliation or seclusion.

Those actions deserving such a protection by nature do not merit the government's attention and vary from a usual visit to a local bar or pub to an innocent a lawful participation in a public gathering, demonstration or participation. The right to anonymity permits to the individual to dissolve with the crowd and though observed to remain anonymous in her actions unless of course he/she is a celebrity. The right to anonymity is especially valuable as far as the political participation of the individual is concerned because not only it protects her in deliberating in the political sphere but it also enables her to form the decision, the choice for such a participation which is otherwise jeopardized. Thus, this right is a precondition to the political autonomy of the individual securing and guaranteeing that she can express her public beliefs, not alone but with others, collectively, without the threat of being manipulated in her political choices or that those will be used against her, in order to cause any discriminations. In this

---

21. See A. Westin, *Privacy and Freedom*, Athenaeum, New York, 1967, p. 31.

22. See Ch. Slobogin, «Public privacy: Camera Surveillance of public places and the right to anonymity», *Mississippi Law Journal*, 2002, pp. 231-315 (239).

frame, the right to anonymity or to public privacy goes beyond the right to privacy of the individual and is tightly bonded with her freedom to enjoy political autonomy, without pressures or interventions by the government authorities.

The theoretical justification of such right is twofold. First, it is based in an approach of the right to privacy that understands it both as a *negative* and as a *positive* freedom.<sup>23</sup> As a negative right, privacy relates to the autonomy of the individual thus fostering for the individual the claim for absence of any interference in her life choices, decision-making or deliberation. From this point, privacy could be represented as the *metaphorical space* that provides the individual with the necessary freedom and autonomy in order to shape his/her views and values without interventions or pressures. Shielded in this metaphorical space the individual can form her decisions regarding not only the private but also the public sphere, and thus make the decision to participate or act in public. As a positive right, privacy relates to the aims, the goals that the individual sets for and tries to achieve under the protective veil of privacy. These goals vary from the protection of intimacy and sexuality of the individual to her communication with the others, the protection of her diversity or the expression of his/her thoughts, feelings, views or values, thus including also political deliberation.

The second part of the theoretical justification of a right to 'public privacy', a right to anonymity, is that otherwise a division between the private and public self of the individual is introduced. Such a division seems not only impossible to be supported in theory but also in practice since it implies that the individual could be divided in two: a public self acting in the open and a private self acting in the intimacy of the private sphere. In theory has justly been supported by Jean Cohen that privacy shields us both in the public, social and private space.<sup>24</sup> A quite similar thesis has been also maintained by the ECHR in its recent jurisprudence.<sup>25</sup> The main argument defending the idea of a unified subject both in public and private is that otherwise the door opens for an inauthentic public life, where the political participation from a civil right and constitutional duty will be transformed to a public *role* of unexpressed intentions and motivations. A right to 'public privacy' should guarantee that no one should be obliged to reveal her

---

23. See I. Berlin, Two concepts of Liberty [1958] in *I. Berlin, Four Essays on Liberty*, Oxford University Press, Oxford, 1969.

24. See J. Cohen, *Regulating Intimacy: A new legal paradigm*, Princeton University Press, Princeton and Oxford, 2004, p. 62.

25. See the ECtHR case of *Kuri and Others v. Slovenia*, 13<sup>th</sup> July 2010, where the ECtHR has supported the idea of 'social privacy' underlining that the immigrants relate socially with the community in which they reside, a bond that falls into the scope of autonomy and the right to privacy as it is protected by the Art. 8 of the ECHR.

private thoughts or views in public but if she decides to do so that she will remain anonymous and thus protected by any discrimination or pressure or social conformity.

## 5. The epimyth of public safety

Should the right to anonymity be considered as a significant component of privacy and thus enjoy its constitutional acknowledgement? For this line of argumentation this choice is central in order to effectively protect the individual against the risks posed to her freedom by the 'Public Camera Surveillance'. The protection of such a right can serve as a guide map for the judiciary in order to perform the principle of proportionality as well as judicial review in the case it clashes with the value of public safety.<sup>26</sup> The augmenting need of protecting public safety in the post-modern, globalized, threatened by terrorism and violence-stricken societies is after all the main reason for the expansion of surveillance, for the creation of a 'panoptic' society in the Foucault's terms.<sup>27</sup> During this transition the boundaries between public and private have shifted in modern societies. A retreat of the public space and a privatization of the public sphere are noted both in Europe and the States mainly due to the use of modern surveillance technology and the Media impact in public life. This change has given rise to arguments that are aiming more and more in understanding the public space less as a sphere for everyone to gather and coexist and more than a place *owned* by all, as a *property*. This notion gives priority to arguments of securing this space in ways that private ownership implies, arguments that mainly are based on communitarian rather than libertarian perspectives. This is the main reason why such policies hierarchize the need for public safety as prior to the enjoyment of the private and public autonomy of the individual.

In concluding, someone could wonder: isn't the need for protecting public safety in today's postmodern, 'risk societies' a solid justification for limiting the freedom and political autonomy of the individual? We must remark that public safety and freedom, private and public autonomy are equally important values and as such should not be hierarchized in their protection. Moreover, the greatest risk posed in the case of justifying the 'Public Camera Surveillance' lays in the creation of a misleading division between the 'good' and the 'bad' citizen. This division preserves the modern 'myth' of public safety and emphasizes that if one is a totally legitimate citizen, acting in a lawful way, no kind of surveillance can harm her.

---

26. See Ch. Slobogin, Proportionality, privacy and public opinion: A reply to Kerr and Swire, *Minnesota Law Review*, 2010, pp. 1588-1619.

27. See M. Foucault, *The Foucault Reader*. (edit. P. Rabinow), Penguin Books, London, 1991.

Not only is this myth leading, since even innocent activities can implicate future risks and discriminations for the individual, fragmenting her autonomy but it is also harmful for a society's common solidarity and *ethos*. It can produce a culture of surveillance among the citizens' themselves who are capable of providing the preconditions for the creation of a totalitarian global society.<sup>28</sup>

---

28. See M. Foucault, *Security, Territory, Population. Lectures at the Collège de France, 1977-78*, (trans. G. Burchell), Palgrave Macmillan, Hampshire 2007.

# **Social Network Sites (SNS): a harmless remarkable technological phenomenon or a harmful backdoor with long-term unpredictable consequences?**

---

---

**Konstantina Alexopoulou**

---

---

## **Introduction**

The vast digitization and the unprecedented dematerialization of copyrighted goods has led to the development of massive online piracy. Facing the ubiquitous issue of online piracy, governments now encounter the possibility of involving Internet intermediaries into the copyright enforcement mechanism by mandatory or voluntary graduated response mechanisms. From an economic point of view, graduated response mechanisms are cost-effective, while any battle against counterfeiting and online piracy seems utopic and inefficient without internet intermediaries' help. Nevertheless, imposing active-preventative rather than passive-reactive obligations on intermediaries may conflict with principles of network neutrality. Policy shift regarding online copyright enforcement requiring from Internet intermediaries activity rather than passivity has significant implications over network neutrality.

In the light of hailing technological evolution, data is processed in new different ways, giving rise to data protection issues that need to be addressed. It is not only a question of quality of data exchange, but also of quantity. Due to new information technologies, enormous quantities of data are being exchanged daily on a worldwide scale, representing threats for intellectual property violations and data protection safeguards. Under the Lisbon Treaty, data protection is strengthened within EU countries providing at the same time a valid legal basis for individuals. Any data controllers should proceed in data processing in conformity with the principles of necessity, purpose limitation and proportionality. Limitations to the exercise the data protection right are feasible if they are exceptional, duly justified and never affect the essential elements of the right itself.

On the other hand, privacy is no longer a social norm, according to Facebook founder Mark Zuckerberg; such argument justifies the unexpectedly high rise of social media these last years, reflecting the evolution in ordinary people's atti-

tudes. Such argument also serves as a perfect excuse for the recent modifications of privacy settings in Facebook<sup>1</sup>.

The following analysis outlines the debate on the nature of information shared on SNS, while stressing out the numerous privacy and security risks that have emerged for SNS users in the digital environment, especially through the use of mobile phones. The recent international jurisprudence enlightens the various aspects of privacy issues that arise, as well as the conflict between the right of privacy and free expression on the one hand and intellectual property rights on the other. This paper also highlights the legal framework regarding ISPs globally, as well as recent legal instruments adopted worldwide in relation to copyright enforcement in the digital environment, providing for a more active participation of ISPs.

## **I. The nature of information contained in SNS: public or private?**

A cutting edge issue arising nowadays refers to the nature of information contained within social network sites such as Facebook or Twitter. A discussion regarding the nature of information available on Facebook should start from Facebook's cornerstone "Facebook is about sharing". Hence, a digital tool created to enable content and data sharing between people, inevitably considers information as public. Facebook is now part of everyday's life of more than 550 million persons, while in 2007, it was used only by 70 million persons. Facebook is also the largest photo sharing application on the web with more than 14 million photos uploaded daily. Thus, Facebook proved to be as a tool flexible, dynamic and socially compelling. As a matter of fact, the default privacy setting in Facebook is "Everyone", entailing that everyone on the Internet including people not logged into Facebook, may access information set to "Everyone", this data being publicly available information. It must be noted that, according to Facebook's Privacy Policy, everyone, by using Facebook, consents to having his personal data transferred and processed in the U.S. It is interesting though that US Courts refrain from broadly concluding that privacy overrides procedural obligations such as the production of evidence.

The security risks emerging for SNS users are enormous as technological evolution creates new means of access and communication which may lead to various infringements. It is crucial to note that according to Facebook Terms and Conditions, which each user has to accept in order to create a Facebook account, a user by posting photos or videos on Facebook (Intellectual Property Content), grants

---

1. [www.guardian.co.uk/technology/2010/jam/11/facebook-privacy](http://www.guardian.co.uk/technology/2010/jam/11/facebook-privacy).



Facebook “a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that he posts on or in connection with Facebook ; this license ends when the user deletes this IP content or his account”. This entails that Facebook (or any third person authorized by Facebook) may use our photos or videos or any other IP content without notice and of course without remuneration, even if Facebook sells such content to third parties. Another interesting detail proving to appear somehow scaring is that a user’s content may be used by Facebook even after the user deletes his Facebook account, if such content still appears on other people’s pages.

According to the above analysis, photos posted on social networking sites become public. Even though published photos remain the property of the user who posted them, in some cases, the courts have held that no breach of the right of privacy occurred when a third party uses pictures already posted on Facebook. Precisely, in the famous Zahia case in France, a French magazine (VSD) published photos of a famous escort girl (Zahia), taken from her Facebook account, where those pictures were accessible to everyone without her consent. Zahia sued the magazine claiming that an infringement of her privacy right as well as an infringement of her right to her image has taken place. But the court decided that since the girl’s photos were directly associated with ongoing judicial proceedings with enormous publicity where she participated, no breach of the privacy right of the right to her image had taken place<sup>2</sup>.

Recently, a French Court condemned a young hacker in five months prison because he had intruded the Twitter accounts of American stars and politicians<sup>3</sup>.

An interesting financial settlement between Courtney Love and a designer on defamation grounds proved how powerful social media sites may be. The famous rock star had made false statements about the designer on MySpace and Twitter. The designer sued Courtney Love leading to a settlement of \$430.000 which according to the designer’s lawyer was “the most powerful admission of wrongdoing”<sup>4</sup>.

### 1) US Jurisprudence

Up to now, social network content did not constitute public data; nevertheless recent US jurisprudence provides the possibility of allowing the use of such data

---

2. [www.voici.fr/potins-people/les-potins-du-jour/zahia-perd-son-proces-face-a-vsd/354623](http://www.voici.fr/potins-people/les-potins-du-jour/zahia-perd-son-proces-face-a-vsd/354623), [www.lefigaro.fr](http://www.lefigaro.fr).

3. [http://www.huffingtonpost.com/2010/03/25/twitter-hacker-that-hit-o\\_n\\_512800.html](http://www.huffingtonpost.com/2010/03/25/twitter-hacker-that-hit-o_n_512800.html).

4. <http://newsinfo.inquirer.net/inquirerheadlines/nation/view/20110306-323732/Courtney-Love-says-sorry-pays-430K-in-Twitter-row>.

in court proceedings. Under the New York Supreme Court, the defendant failed to establish a factual predicate with respect to the relevance of the evidence. “Indeed, defendant essentially sought permission to conduct a «fishing expedition» into plaintiff’s Facebook account based on the mere hope of finding relevant evidence”<sup>5</sup>. The New York Supreme Court validated the trial’s court denial to compel disclosure of the plaintiff’s Facebook account in a personal injury action. However, the Supreme Court did not go as far as to confirm the issuance of a protective order for the plaintiff as did the trial court, preventing the defendant from ever seeking the Facebook data.

This decision allows in the future the issuance of an order enabling access to social networking data, if a relevant request is well justified. Until recently, litigants did not realize the importance of information contained in social networking sites. In a recent case where the plaintiff sought damages for personal injuries and loss of enjoyment of life, the defendant requested and the Court granted an order for access to the plaintiff’s Facebook and MySpace accounts to gather evidence contradicting the plaintiff’s arguments. Indeed, the plaintiff had posted pictures and other public postings that proved she was capable of traveling and working, thus the Court held that these public postings justified the defendant’s request, considered as relevant and reasonable<sup>6</sup>. This ruling ordered the plaintiff to give the defendant direct access to log in and view her Facebook and MySpace accounts.

Several recent US rulings tend to consider postings on Facebook public and deny protective orders for Facebook, MySpace and meetup.com pages, ordering the discoverability of such information<sup>7</sup>. The California Court of Appeal characterized the plaintiff’s MySpace post as public, even though the plaintiff deleted it after posting it, thus rejecting a law suit claiming invasion of privacy because the defendant had re-post the initial plaintiff’s post<sup>8</sup>. On the contrary, the US District Court in Nevada denied a motion requesting to force the plaintiff to allow direct access to her Facebook and MySpace accounts. This case involved claim of sexual harassment at work which led to the plaintiff’s suicide attempts after quitting her job. The defendant argued that the plaintiff listed herself as single while married into MySpace, arguing that such finding affects the plaintiff’s credibility. The Court refused by ruling, stating that the defendant’s arguments represented only

---

5. *Mc Cann v. Harleyville Insurance Company of New York*, 20b N.Y App.Div.LEXIS 8396 (Nov. 12, 2010).

6. *Romano v. Steel case Inc.*, 907 N.Y.S. 2d 650 (2010).

7. *Ledbetter v. WalMart Stores Inc.*, 2009 U.S. Dist. LEXIS 126859, at 4-5 (D.Colo.Apr.21, 2009).

8. *Moreno v. Hanford Sentinel Inc.*, 172 Cal. App.4<sup>th</sup> 1125, 1130-31 (2009).

“suspicions or speculations as to what information might be contained in the private messages<sup>9</sup> and characterized the defendant’s request as “fishing expedition”.

Up to now, the US case law has made no general findings about the discoverability of social networking data depending on the nature of the cases or the way the discoverability request is made (directly from the litigant or via the social networking site).

Furthermore, a recent US ruling ruled on the nature of a posting on SNS and held that a posting without the author’s consent constituted a breach of state law but not of privacy. More precisely, an employer who allegedly posted to an employee’s Facebook and Twitter accounts without her consent faced liability for its actions, according to a federal judge in Illinois<sup>10</sup>. The plaintiff worked as the Director of Marketing, Public Relations and E-Commerce for an interior designer and the plaintiff contended that she created a “popular personal following” on Facebook and Twitter and that she also created a company blog called “Designer Diaries”. In September 2009 she had an accident and she was hospitalized for months. During this time the defendant impersonated Maremont by writing Posts and Tweets to her personal Facebook and Twitter followers promoting their company. And even after Maremont asked the Defendants to stop, they continued until she finally changed her account passwords. The court ruled that Maremont had adequately alleged a commercial injury based on the defendants’ deceptive use of her name and likeness and that they used her likeness to promote the business without her written consent in the violation of also state law but the court ruled that the Maremont had not adequately developed her alternate argument that defendants’ intrusion into her personal “digital life” is actionable under the common law theory of unreasonable intrusion upon the seclusion of another. The case is now proceeding to discovery.

As this case demonstrates, social media litigation is a growing trend. Employers may unwittingly expose themselves to claims by assuming that all online activity related to the business is company property. Employers should clearly distinguish between the personal social media accounts of their employees and those that belong to the business itself. Personal employee accounts, even if used to promote company business, should not be accessed without the employees’ express written permission. Clear written policies on social media use are the best way to clarify the respective roles and expectations of employees and employers.

---

9. *Mackel Prang v. Fidelity National Title Agency of Nevada Inc.*, 2007 US Dist. LEXIS 2379 (D.Nev. Jan.9,2007).

10. <http://www.huntonlaborblog.com/2011/03/articles/employment-policies/look-before-you-tweet-employer-may-be-liable-for-impersonating-employee-on-facebook-twitter/>.

## 2) Common law jurisprudence

The increasingly decisive role of Facebook in communications is undisputed. According to a 2009 Australian judgment, Facebook was a legally viable way to communicate, even regarding legal documents. The Canberra Supreme Court affirmed a request to serve legal documents via Facebook after repeatedly failing to serve the papers in person<sup>11</sup>.

According to a Canadian Court, a litigant could not have serious expectations of privacy given that 366 people had already been granted access to his private site<sup>12</sup>. In this case, the plaintiff, after a serious car accident, sued the car driver seeking damages for the detrimental impact on her enjoyment of life and her inability to participate in social activities. The defendant's attorney discovered (before the trial) a public website with the name of the plaintiff, containing post-accident pictures of the plaintiff at a party as well as a Facebook account with the plaintiff's name and list of 366 Facebook friends; due to privacy settings that the plaintiff had set, access to her Facebook page was restricted. Thus, the opposing party sought for a court order imposing production of Facebook pages potentially containing relevant information. Despite the plaintiff's objection arguing that the defendant was on a "fishing expedition", claiming that only speculations on the real material on the site existed, the judge ordered Facebook pages to be produced, arguing that since Facebook is a SNS where a large amount of photos are posted by its users, it was reasonable to assume that there would be relevant photos on the plaintiff's pages.

Another interesting decision dealing with the production of the access-limited contents of a Facebook profile is the one based on *Leduc v. Roman* case<sup>13</sup>, in which the plaintiff sought damages due to a car accident, claiming suffering various ailments and loss of enjoyment of life. The opposing party discovered the plaintiff's Facebook account, to which access was allowed only to his Facebook friends and requested an order requiring the preservation of all information on Facebook profile and the production of the Facebook profile itself. The plaintiff argued once again that the mere existence of a Facebook account did not entail that relevant to the case material was posted on his Facebook site, trying to differentiate this case from the *Murphy* case<sup>14</sup>. The court held that "(...) Facebook is not used as a

---

11. <http://www.telegraph.co.uk/news/newstopics/howaboutthat/3793491/Australian-couple-served-with-legal-documents-via-Facebook.html>.

12. *Murphy v. Perger* (2007) oJ. No 5511 2007 WL 5354848 (Ont. S.C.).

13. *Leduc v. Roman*, 2008 CanLII 6838 (ont.S.C.), at para.17 (Leduc).

14. *Murphy*, supra note.

means by which account holders carry on monologues with themselves, it is a device by which users share with others information about who they are, what they like, (...) in varying degrees of detail. A party who maintains a private or limited access Facebook profile stands in no different position than one who sets up a publicly available profile. Both are obliged to identify and produce any postings that relate to any matter at issue in an action. (...). To permit a party claiming very substantial damages for loss of enjoyment of life to hide behind self-set privacy controls on a website, the primary purpose of which is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trial.<sup>15</sup>

Facebook has proved to be a professionally dangerous online tool, since several discharges caused by Facebook postings have been registered: For instance, an employee was fired by the American Medical Response for Connecticut, after the employee posted complaints about her boss on Facebook. The case was finally settled, the main argument being that the online comments constituted protective activity and that the discharge violated federal labor law<sup>16</sup>. In UK, an intern at Anglo Irish Bank was fired after his boss discovered an intern's photo at a Halloween party posted in Facebook while he requested a day off due to "family emergency"<sup>17</sup>.

### **3) European Jurisprudence**

#### **a. French Jurisprudence**

In a recent judgement, the Paris Court of First Instance (Tribunal de Grande Instance de Paris)<sup>18</sup> ordered Facebook France to withdraw a defamatory comment with picture of the Bishop of Soissons and condemned Facebook France to pay a fine of 500€ for each of day of delay in case of non compliance with the decision. Furthermore, the French Court ordered Facebook France to communicate all data permitting the identification of all authors of the defamatory pages as well as to withdraw all defamatory comments on a Facebook page regarding the Bishop and condemned Facebook to pay a fine of 500€ for each of day of delay in case of non-compliance with the decision, because Facebook was considered to have incited racial hatred and have reproduced and hosted unlawful content. Nevertheless, Facebook appealed the decision and its appeal was granted on the

---

15. *Leduc*, supra note, at paragraphs 31-32 & 35.

16. [www.socialnetworkinglawblog.com](http://www.socialnetworkinglawblog.com).

17. [www.facebook.com/nde.php?nde\\_id=126911673991090](http://www.facebook.com/nde.php?nde_id=126911673991090).

18. Ordonnance de Référé du 13.04.2010, Tribunal de Grande Instance de Paris, No RG 10/53340, [www.scribd.com/doc/29980259/OrdonnanceRéférédeParis](http://www.scribd.com/doc/29980259/OrdonnanceRéférédeParis).

grounds that Facebook France was not legalized to appear in Court, since it was only a branch office of Facebook UK, which in its turn was completely independent of Facebook Inc, the US company which is the exclusive editor of the site and the only one controlling the Facebook content. In the meanwhile Facebook France never provided the ordered data, only withdrew the unlawful content.

Two judgments on the same matter at the Council of the “prud’ hommes” of Boulogne-Billancourt November 2010 concluded that the employer who produced a Facebook page of which the wall was accessible to the “friends of the friends” did not violate the private life of the two employees, dismissed for breach of discipline. At the point that this method of access surpassed the private sphere, the council considered that the method of proof based on the grounds of the dismissal, was lawful. Precisely, three employees of the corporation Alten had created a Facebook page the goal of which was to criticize their hierarchy. They had chosen to authorize the access “to friends of friends” and most notably the current and the former employees of the business. They had founded the “club of the harmful”, virtual club at the core of which was to “making fun” of the superior hierarchic one, all day long, without the boss having ever realized anything and for several months. The court held that, while participating in these exchanges, the employees had abused the right of expression, in the framework of the business by the item 1121-1 of the French labor code. They harmed the picture of their business infringing the functions of the service recruitment, thus having an effect on future employees. The Council specified that while choosing this access method, their posts were likely to be read by exterior people to the business. It concluded that the dismissal “for the incitement of the rebellions against the hierarchy and for denigration towards the corporation Alten” relies on a real and serious cause.

### **b. Denmark - The Pirate Bay case**

On 5 February 2008, the district court of Frederiksberg, Copenhagen ruled that one of Denmark’s largest ISPs, DMT2-Tele2, was assisting its customers in copyright infringement by allowing the use of The Pirate Bay, and that they were to block access to the site<sup>19</sup>. Although the ISP had decided to challenge the verdict with support from the Danish Telecommunication Industries Association, they finally complied with it and blocked access to The Pirate Bay. The Pirate Bay reacted by creating an alternate site (with instructions on how to work around the block), while the International Federation of the Phonographic Industry (IFPI) welcomed the block and encouraged other ISPs to follow suit. The verdict was af-

---

19. Decision of 5-2-2008, Bailiff’s Court of Frederiksberg, FS 14324/2007, available at <http://ssrn.com/abstract=1093246>.

firmed in the Eastern High Court of Denmark on 26 November 2008. The Court found it undisputed that the website worked as index and search engine, allowing users of the website to get accessibility to files from each other. On the basis of the production of evidence and argumentation, the court held that an overwhelming part of the material exchanged through the website by the users are protected by copyright, administrated by the claimants and that the claimants had not given permission to the materials publication and accessibility. In addition, it was held that the use of the website had a certain diffusion in Denmark.

Following the court's decision, TDC, Denmark's largest ISP and owner of most of the cables, decided to block access to The Pirate Bay as a preventive measure. Other Danish ISPs have commented that they would prefer not to intervene in their customers' communication, but have reluctantly put the block in effect in order to avoid fines. Tele2's owner Telenor in turn appealed the high court verdict to the Supreme Court of Denmark, which in April 2009 accepted the case for processing.

### **c. Sweden**

In Sweden, in February 2009 the Pirate Bay site's trial began, for copyright infringement. The defendants' sentences imposed on the owners of the site were one year imprisonment and 30 million Swedish kronor (2.7 million euros). In May 2010, The Pirate Bay's Swedish internet service provider finally lost an appeal against an order to stop providing service to the site. Although the service provider had already complied with an earlier order in August 2009 and The Pirate Bay was afterwards hosted elsewhere, in June 2010 the ISP chose also to block their customers from accessing The Pirate Bay in its new location. One of the judges in the case later commented that the court's order did not require the ISP to control their customers' access to the site, but the ISP wanted to avoid any risk.

The Pirate Bay Case caused political development in Sweden, leading to the creation of a political party called "the Pirate Party". The main purpose of the party is to change the legal framework on copyright. It has also expressed different positions on trade and patent rights of users on the Internet. In 2006 the Pirate Bay took part in the general elections in Sweden reaching 0.63%. On May 31, 2006, the Swedish police raided the place occupied by the Pirate Bay, causing the blocking of the page for 3 days. The above raid increased the party's popularity dramatically. In July 2006 the party organized demonstrations in Stockholm and Gothenburg. In February 2009 the Pirate Bay site's trial began, for copyright infringement. Following the disclosure of sentencing in April of that year, members of the party tripled in only one week. It is also remarkable that the Pirate Party took part in the European Elections in 2009, electing a Member of Parliament after reaching 7,1%. The Swedish example gave impetus to other countries

to found similar political parties. Officially, these kind of political parties exist in Germany, Austria, France, Spain, Poland and Finland and unofficially in USA, UK, Denmark, Argentina, Chile, Australia, Nederland's, Portugal, Czech, Slovakia and Slovenia.

#### **d. Greece**

In Greece, in March 2010 one of the administrators of the Greek pirate site "gamato.info" was arrested and sent to the Criminal Court by the Authorities of the Electronic Crime. Surveys of prosecutors began after a complaint lodged by the Society for the Protection of Audiovisual Works. As a result of investigations by the authorities, during the three and a half years of «gamato.info» operation, about 800,000 users, downloaded free in total 3.2 million film titles, music and computer software and the damage caused to the plaintiff company reached 15 million euros.

## **II. Special threats represented by mobile phone access to SNS**

Another relative growing-up phenomenon refers to the increasing percentage of cell phone subscribers using their phone for social networking. Such technological development has been facilitated thanks to global positioning satellites permitting to trace a cell phone, while more and more SNS seek to capitalize on location information, providing services such as showing to users where friends are in real time. Almost 134 million mobile users are estimated to access the SNS in Europe in 2012, most of them being largely unaware of security and privacy risks. Mobile users are exposed to many privacy threats such as identity theft, malware, corporate data leakage, device theft, user's position tracking and data misuse.

Efficient hackers may easily take control of a user's security credentials and then proceed to take full control of the user's account by modifying his setting, by posting malicious comments or even by spreading malicious software<sup>20</sup>. Another serious security risk includes the distribution of malware either through Facebook and Twitter or through the mobile itself, infecting the phone's contacts as well as SNS contacts. It is possible that an infected computer will post a link containing malicious software, where users click, trusting the friend who posted it, not being aware that their friend has been hacked. One of the most "advanced" techniques used by hackers includes the creation of Twitter new accounts regarding the trendiest topics discussed on Twitter at that time and the posting of re-

---

20. ENISA "Security issues in the context of authentication using mobile devices (mobile eID), 2008, <http://www.enisa.europa.eu/act/it/eid/mobile-eid/?searchterm=security>.



lated messages. Such messages are contained in Twitter search results, leading unsuspecting users operating these searches to click on the infected link.

Another frequent phenomenon consists of the spread of business information through SNS leading to unauthorized disclosure of corporate sensitive data, affecting not only user's privacy but also professional reputation<sup>21</sup>. According to the Working Party of Art.29, Directive 95/46/EC on data protection<sup>22</sup> is also applicable to SNS providers even if their headquarters are located outside of the European Economic Area. Pursuant to an Opinion issued by the aforementioned Working Party on Online Social Networking (Opinion 5/2009 on online social networking 12-6-2009)<sup>23</sup>, SNS providers are data controllers under the above Directive and on this purpose are recommended to remind SNS users that uploading information about other individuals may violate their privacy and thus, it should be done only with the individual's consent, offer privacy-friendly default settings to reduce the risk of unlawful processing by third parties and make aware SNS users about the privacy risks to themselves and to others when they upload information on the SNS. In other words, the real-time spread of data and information through SNS entail at the same time enormous benefits but can also cause serious damages, threatening users' privacy and personal and professional reputation. It seems that the most secure defence is awareness raising, since technical safeguards may prove to be easily out-to-date.

### **III. The role of ISPs regarding privacy and security issues in relation to SNS**

#### ***a) Existing legal framework***

Up to very recently, the principle of network neutrality regarding the role of Information Service Provider (ISP) prevailed globally, while no general obligation of monitoring hosted or transmitted content existed for ISPs in most legislations worldwide.

More precisely, according to the Art.(2a) of Directive 2000/31<sup>24</sup> "any service normally provided for remuneration at a distance, by electronic means and at the

---

21. <http://www.dailymail.co.uk/news/article-1082437/BA-check-staff-post-comments-smelly-passengers-Facebook.html?To=1490>.

22. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995.

23. [http://ec.europa.eu/justice\\_home/fsa/privacy/workinggroup/wpdocs/2009.en.htm](http://ec.europa.eu/justice_home/fsa/privacy/workinggroup/wpdocs/2009.en.htm).

24. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000.

individual request of a recipient of services” constitutes information society services. All issues regarding ISPs’ liability are addressed in Art.12-15 of the above Directive. In art. 12 & 13<sup>25</sup>, the Directive provides the conditions that need to be met for the exemption of an ISP from liability concerning the activities of mere conduit and caching while art.14 of the same Directive provides for the exemption from liability when the activity consists of storage of information.

Thus, under to EU law, an ISP is totally exempted from liability in case his activity is merely technical, automatic and passive, proving the absence of knowledge or control of the (data) information transmitted or stored in its communication network. This only refers to the activities of “mere conduit” and “caching” as explicitly analyzed in art. 12 and 13 of Directive 2000/31/EC. Regarding activities such as the storage of information, the ISP is not liable if he has not actual knowledge of illegal activity or information and upon obtaining such knowledge or awareness, he acts expeditiously to remove or disable access to the info. While hosting of information may benefit from an exemption if the requirements set out by Art.14 of 2000/31/EC are met, the ISP may incur potential criminal law or damage liability. According to an interpretation of “actual knowledge” of Art.14(1) of 2000/31/EC, a mere suspicion or assumption regarding the illegal activity would not be sufficient to fulfill the requirements “actual knowledge” but includes only past and present information, activity or facts indicating illegal activity. In light of the above, it must be noted that in many Member States the liability of a service provider, based on art.12,13,14 of Directive 2000/31/EC, would be excluded because of the lack of the subjective fault.

The principle of “notice and take down” is established by Art.14(1)(b) of Directive 2000/31/EC according to which “where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: [...] (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.”

The limitations to that principle are set out by Recital 46 of this Directive, which provides that the principle of freedom of expression and of procedures established for this purpose at national level should be observed when enforcing the removal or disabling of access.

The Directive does not constrain member states to impose a general obligation on ISPs to monitor the information they transmit or to store or to seek the information they transmit or store or to seek actively facts or circumstances indicating

---

25. Supra note 24.

illegal activity. Nevertheless, member states may establish obligations for ISPs to inform promptly the competent public authorities of the alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

At the same time, in case of infringement in relation to hosting activities, (storage of information), a national Court or administrative authority may request the ISP to terminate or prevent such infringement; member states may simultaneously establish procedures governing the removal or disabling of access to such infringing information<sup>26</sup>.

On this purpose, the Greek Law, transposing the above Directive<sup>27</sup>, provides that ISPs are obliged to inform promptly the competent Greek authorities in case of alleged illegal information or activities undertaken by recipients of their service and to announce to the competent authorities at their request information facilitating the identification of recipients of their service with whom they have storage agreements<sup>28</sup>.

In addition to the Directive 2000/31, EU has enacted Directive 2004/48/EC<sup>29</sup>, pursuant to the provisions of which, member states shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the IP rights covered by this Directive. Those measures shall be fair and equitable and shall not be unnecessarily complicated or costly entail unreasonable time-limits or unwanted delays. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive<sup>30</sup>.

Furthermore, the above Directive ("the Enforcement Directive") also provides that in case of issuance of a judicial decision finding an infringement of an IP right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement (...) and right holders may apply for an injunction against intermediaries whose services are used by a third

---

26. Art. 14§3 Directive 2000/31/EC, *supra* note 24.

27. Π.Δ 131/2003, ΦΕΚ Α' 116/16-05-2003.

28. Art. 14 Π.Δ 131/2003.

29. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of Intellectual Property Rights, Official Journal of the European Union L 157 of 30 April 2004.

30. Art. 3 General Obligation, Directive 2004/48/EC, *supra* note 25.

party to infringe an IP right<sup>31</sup>. Most of the provisions of Directive 2004/48/EC were transposed in Greek law through Law 3524/2007<sup>32</sup>.

Pursuant to Art. 8 of the Directive 2004/48/EC, member states shall ensure that competent judicial authorities may order that information on the origin and distribution networks of the infringing goods/services shall be provided by the infringer and/or third parties found in possession of the infringing goods on a commercial scale or found to be using the infringing services or found to be providing on a commercial scale services used in infringing activities or being indicated as being involved in the production, manufacture or distribution of the said good or services. Thus, the Directive aims at detecting all actors involved in IP infringements, including intermediaries such as ISP, in contrast to TRIPS Agreement, which provides for an option of Member States to grant judicial authorities “the authority to order the infringer to inform the right holder of the identity of third persons involved in the production and distribution of infringing goods<sup>33</sup>. By choosing such wording, the Directive enables the disclosure of information regarding all persons involved in the infringing activities, trying to trace them without the help or cooperation of the infringer. Furthermore, according to Art.11 of Directive 2004/48 in cases where a third party is using the services of an intermediary to infringe an IP right but the true identity of that infringer remains unknown, an injunction may be given against an intermediary requiring the prevention of the continuation of a specific act of infringement as well as the prevention of repetition of the same or similar infringement in the future, under the condition that the principles of efficacy, dissuasiveness and proportionality are met. All conditions and procedures relating to such injunctions should be defined in national law.

According to EU authorities, the right to obtain information from third parties as provided in the Enforcement Directive was not transposed uniformly within EU: some member states have created a special procedure providing for a right of information as a provisional measure, other member states have conformed with the Directive, limiting such right only in the context of judicial proceedings. Under the findings of the Commission Report, an almost unanimous conclusion on the Enforcement Directive, seems to be that “after the transposition of the Directive, national Courts have seen a significant increase in request for information”, help-

---

31. Art.11 Directive 2004/48/EC, *ibid*.

32. ΦΕΚ Α' 15/26-01-2007.

33. Art.47 TRIPS AGREEMENT, Agreement on Trade-Related Aspects of Intellectual Property Rights, [http://www.wto.org/english/tratop\\_e/trips\\_e/t\\_agm0\\_e.htm](http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm).

ing to trace infringers easier,<sup>34</sup> especially directed towards ISPs. Unfortunately the enforcement Directive did not produce impressive results, since damages awarded in IP rights cases did not reflect significant increase after enacting the Directive<sup>35</sup>. Further, right holders complain arguing that nowadays the level of profit made by an IP infringement is substantially higher than the actual compensation awarded by the Courts. Thus, the Commission estimates that courts should possibly review the calculation of damages awarded to right holders, so as to take into account the unjust enrichment of the infringers to the detriment of the right holders. It must be stressed out that, according to the Commission Staff Working Document<sup>36</sup>, accompanying the above Report, Greece has not transposed the Directive in its entirety yet and major Member States were late with the transposition procedure (France, Germany, Sweden and Portugal).

Another crucial remark pointed out by several member states is the growing difficulty in gathering evidence for infringements committed via the Internet and the insufficiency of the Directive to address this issue. Special reference is made to Greece, where many requests made by right holders for Court orders have been rejected as “vague”, when right holders are not able to specify exact details regarding such evidence. It must be noted, finally, that many provisions of the Enforcement Directive set out stricter and broader obligations than the ones provided by TRIPS Agreement<sup>37</sup>, where some legal issues are not even covered.

Various data protection and privacy issues are also raised in relation to traffic management policies. ISPs participate in “traffic management” by collecting both content and traffic data of individuals. It is quite obvious and rather easy for an ISP to block or to examine each message or information sent over a network, since each communication is associated to a certain IP address.

First of all, traffic management mechanism may breach the confidentiality of communications guaranteed by Art. 8 of European Convention for Protection of Human Rights and Fundamental Freedoms and Art. 7 & 8 of the Charter of Fundamental Rights of EU. Currently, the e-Privacy Directive<sup>38</sup> requires consent

---

34. Commission staff working Document, 22.12.2010, COM (2010) 779 final.

35. Report from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions, Application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights SEC(2010) 1589 final.

36. Supra note 30.

37. Supra note 29.

38. Art 5 § 1, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, OJ L 201, 31.7.2002.

to enable “....listening, tapping, storage or other kinds of interception or surveillance of communication (...) by persons other than users. The only exemption to this provision is subject to a severe application of the proportionality principle, in order to prevent, investigate, detect or prosecute criminal offences or unauthorized use of the electronic communication system or in order to safeguard national security, defence, public security. Only security reasons justify the by-passing of the user’s consent, as provided in Art. 4 of the e-Privacy Directive<sup>39</sup>. Consent must be informed, specific and freely given. Such consent needs to be express and the user must be aware about the purposes of the traffic management policies. Furthermore, the user must be able to understand the language used by the ISP and to understand what he is consenting to and for what purposes.

The proposal of EDPS<sup>40</sup> offering an alternative choice to users, such as internet subscriptions not subject to traffic management, does not seem to provide a viable solution, because it does not handle cases that need special treatment: users tending to breach law and use illegal content, for instance, will not choose of course to be subject to constant data monitoring. It is crucial to highlight that in case of content, according to art. 5. 1 of e-Privacy Directive<sup>41</sup>, all users concerned shall provide their consent and not only the user sending content, which creates inevitably a dead-end situation.

Finally, the provisions of the Directive 2006/24/EC<sup>42</sup>, are only applicable in the field of protection of IP if the offence has a criminal dimension, not applying to the content of electronic communications.

Recently, the Committee of experts on New Media of the Council of Europe has issued draft recommendations<sup>43</sup> and guidelines<sup>44</sup> regarding the protection of human rights by search engines and social networking providers. Some of the main

---

39. Supra note 34.

40. EDPS comments on Net Neutrality and Traffic Management/6-10-2010, available at [http://ec.europa.eu/information\\_society/policy/ecomms/doc/library/public\\_consult/net\\_neutrality/comments/04eu\\_national\\_regional\\_ministries\\_authorities\\_incl\\_berrec/edps.pdf](http://ec.europa.eu/information_society/policy/ecomms/doc/library/public_consult/net_neutrality/comments/04eu_national_regional_ministries_authorities_incl_berrec/edps.pdf).

41. Supra note 34.

42. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105/54 13.4.2006.

43. [http://www.coe.int/t/dghl/standardsetting/media/mcnm/MC-NM\(2010\)003\\_en%20Draft%20Rec%20%20SNS.asp#TopOfPage](http://www.coe.int/t/dghl/standardsetting/media/mcnm/MC-NM(2010)003_en%20Draft%20Rec%20%20SNS.asp#TopOfPage).

44. [http://www.coe.int/t/dghl/standardsetting/media/mc-nm/MC-NM\(2011\)008\\_enGuidelines%20for%20soc%20Netw%20prov.asp#TopOfPage](http://www.coe.int/t/dghl/standardsetting/media/mc-nm/MC-NM(2011)008_enGuidelines%20for%20soc%20Netw%20prov.asp#TopOfPage).

recommendations state that the member states, in cooperation with the private sector actors and civil society, are recommended to develop and promote coherent strategies to protect and promote respect for human rights with regard to social networking services, in particular 1) by ensuring users are aware of possible challenges to their human rights on social networking services as well as on how to avoid having a negative impact on other people's rights when using these services; 2) by protecting users of social networking services from harm by other users while also ensuring all users' right to freedom of expression and access to information. Also, 3) by encouraging transparency about the kinds of personal data that are being collected and the legitimate purposes for which they are being processed, including further processing by third parties and by preventing the illegitimate processing of personal data. In the field of users control over their data the committee recommends that the default setting for users should be that access is limited to self-selected friends; that the users are informed about the need to obtain the prior consent of other people before they publish their personal data, in cases where they have widened access beyond self-selected friends.

### ***b) ECJ jurisprudence***

Up to now, the European Court of Justice (ECJ) has not issued an *ad hoc* decision regarding the role of ISPs in relation to SNS. Thus, recent ECJ jurisprudence related to ISPS may serve as an enlightening example of future *ad hoc* decisions.

According to the ECJ, "a fair balance should be struck between the various fundamental rights protected by the Community legal order"<sup>45</sup>, more precisely between the right to property, including IP rights and the right to data protection, both constituting fundamental rights directly recognized and expressly protected by the Charter of Fundamental Rights of the EU<sup>46</sup>. Nevertheless, none of the ECJ judgements entail that either right prevails over the other.

Under ECJ case law<sup>47</sup>, ISPs may incur "secondary liability" or "accessory liability", referring to the possible liability of an ISP for infringement committed by users of the service. Furthermore, if the service provider has actual knowledge of illegal activity and is aware of facts or circumstances from which the illegal activity is apparent and upon obtaining such knowledge, does not act expeditiously to

---

45. Judgment of 29-01-2008 in the case C-275/06.

46. Art.7,8,17(2), Charter of Fundamental Rights of EU, also available at [http://www.europarl.europa.eu/charter/default\\_en.htm](http://www.europarl.europa.eu/charter/default_en.htm).

47. C-324/29, OJ C 267 of 07.11.2009, p.40.

remove or to disable access to (infringing) info, then it will be held liable for such infringement on the legal grounds of Art. 12, 13, 14 of Directive 2000/31<sup>48</sup>.

Regarding ISP liability, the notion of “actual knowledge” of the ISP, as contained in Art. 14(1) of 2000/31/EC, does not entail a mere suspicion or assumption regarding the illegal activity. Nevertheless, it is interesting to follow the analysis of the Advocate General in Case C-324/09, who argues that if the ISP provider is notified about an IP infringement and the same user continues or repeats the same infringement, then the notion of “actual knowledge” is concluded and the exemption from liability for the ISP does not apply<sup>49</sup>. It remains to wait whether the Court will approve such approach.

Another anticipated judgment will be the one in case C-461/10, where the Swedish Court requested for a preliminary ruling on (the question) whether Directive 2006/24/EC amending Directive 2002/58/EC (the data storage Directive) precludes the application of a national provision based on Directive 2004/48/EC (the Enforcement Directive), according to which an ISP may be ordered to give a copyright holder information on a subscriber in civil proceedings, thus facilitating the identification of a particular subscriber claimed to have committed an infringement. In the same reference the Swedish Court also asks whether the fact that the member state has not implemented the data storage Directive despite the fact that the period prescribed for implement action has expired, has any impact on the above ruling<sup>50</sup>.

At the same time, the ECJ is called to rule whether Directives 2001/29 and 2004/48 in conjunction with Directive 95/46, 2000/31, 2002/58 permit Member States to authorize a national Court before which substance proceedings have been brought, to order a hosting ISP to introduce for all its customers in abstracto and as a preventive measure at its own cost and for an unlimited period, a system for filtering most of info stored on its servers in order to identify on its servers electronic files containing musical, cinematographic or audiovisual work in respect of which SABAM claims to hold rights and subsequently to block the exchange of such files<sup>51</sup>.

### *c) Australian Jurisprudence*

The Common Law countries have already faced many cases of ISP liability, among which one of the most interesting is the one issued by the Federal Court

---

48. Supra note 24.

49. <http://curia.europa.eu/jcms/upload/docs/application/pdf/2010-12/cp100119en.pdf>.

50. Case C-406/10, 2010/C 317/42, OJ 2010 C/317/24.

51. Case C-360/10, 2010/C, 288/30, OJ 2010, C288/18.



of Australia that held in a recent judgement<sup>52</sup> that an ISP (namely “iiNet”) was not responsible for copyright infringement undertaken by their customers. In this case, ISP’s customers infringed copyright. The question was whether iiNet authorized that infringement, by failing to taking any steps to stop infringing conduct. Nevertheless, according to the Australian Court, the knowledge of the infringement by the ISP and the absence of any act to stop it did not entail “authorization”, because the provision of Internet access constitutes a precondition and not the “means of the infringement”. The Court also held that the mere use of the Internet did not establish *per se* an infringement to copyright holders. Pursuant to the Court analysis, the “means” of infringement encompassed the electronic mechanism used to distribute large quantities of data, over which the ISP had no control at all. The Australian Court also held that national law does not allow the notification, suspension and termination of customer accounts, as a relevant measure to prevent copyright infringement. The Court goes further to its analysis stating that unlike the decisions in Kazaa and Cooper, iiNet did not deliberately favour, approve or countenance copyright infringement, because it did not deliberately proceed to any act to achieve an infringing activity. The Court concludes that “an ISP such as iiNet provides a legitimate communicational facility which is neither intended nor designed to infringe copyright”<sup>53</sup>. The above case resulted in a landmark judgement with great interest for the whole motion picture industry. The applicants in the Federal Court proceedings included 33 motion picture companies among which Universal Studios, Paramount Pictures, Warner Bros, Disney, Columbia Pictures, Twentieth Century Fox, Village Road Show, NBC Studios, etc.

This judgment was recently appealed by RoadShows Films leading to a dismissal<sup>54</sup> of the appeal. The Court ruled that the ISP conduct did not amount to authorization of the primary acts of infringement on the part of iiNet users. Nevertheless, the Court held that ISPs can be found liable for authorizing their users for infringement under specific circumstances, namely if ISP has been provided with “unequivocal and cogent evidence of the alleged primary acts of infringement” by use of the ISP service in question and copyright owners had proven that they had undertaken to reimburse ISP for the reasonable cost of verifying the particulars of

---

52. *Road Show Films Pty Ltd v iiNet Limited* (n3) [2010] FCA 24, (04.02.2010), [www.austlii.edu.au/au/cases/cth/FCA/2010/24.html](http://www.austlii.edu.au/au/cases/cth/FCA/2010/24.html).

53. As the ISP did not create and did not control the system mechanism allowing the film copying and the mere failure to terminate users, accounts did not signify authorization of copyright infringement.

54. *Road Show Films Pty Ltd v iiNet Limited* [2011] FCAFC 23 (24.02.2011), [www.austlii.edu.au/au/cases/cth/FCAFC/2011/23.html](http://www.austlii.edu.au/au/cases/cth/FCAFC/2011/23.html).

the primary acts of infringement and of establishing and maintaining a regime to monitor the use of the ISP service to determine whether further acts of infringement occur and to indemnify ISP in respect of any liability reasonably incurred by ISP, as a consequence of mistakenly suspending or terminating a service on the basis of allegations made by copyright owners”.

Apart from other comments, it is crucial to underline the reserve of the judgement on ISP's liability regarding future infringements. As judge Emmett held “It does not necessarily follow from the failure of the present proceeding that circumstances could not exist whereby iiNet might in the future be held to have authorized primary act of infringement”<sup>55</sup>.

#### ***d) Italian Jurisprudence***

In February 2010 an Italian court in Milan found three Google executives guilty of violating Italian privacy laws. The executives were accused for allowing a video showing an autistic teenager being bullied to be posted online. The Google executives were fined and received six-month suspended jail sentences. Richard Thomas, the UK's former Information Commissioner and Senior Global Privacy Advisor to Hunton & Williams said that the case is “ridiculous” and “it is unrealistic to expect firms to monitor everything that goes online.” New York Times reported on this case “The court found that Google had an obligation to make users more aware of its EU privacy policies and cited Google's active marketing of its Google Video site as indicative of the company's profit motive for not removing the video sooner.”

### **IV. Notice and take down regime**

Since the Enforcement Directive is not obliging member states to adopt specific provisions regarding the issuance of conditions of injunctions against intermediaries, it is left at the discretion of each State to determine when and how an injunction can be issued against an intermediary. Most national legislations do not involve intermediaries to the injunction procedure. The Commission in its recent Report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions<sup>56</sup>, seems rather favourable regarding the application of “notice and take-down” policy, supporting the view that injunctions should not depend on the liability of intermediaries and that intermediaries should be more involved to the above injunction procedure.

---

55. Supra note 45.

56. Supra note 35.

It is crucial to note that supporters of graduated response systems argue that such systems are well justified on economic grounds because of the obvious reduction of litigation costs associated with copyright enforcement. The US experience shows that only few copyright infringement cases were finally brought to courts, while the majority led to out-of-court settlements with insignificant gain for the plaintiff's (copyright holders), since the fines imposed did not prove to be threatening for IP infringers<sup>57</sup>.

Notice and take down procedures are already functioning in Finland, France, US, and Canada and relevant legislation has been enacted but not yet implemented in New Zealand, Spain and UK.

#### ***a) HADOPI Law- France***

The modified version of Hadopi Law, finally approved by the French Constitutional Council, secures the fair trial principle by vesting the judge with the authority of subscriber accounts termination<sup>58</sup>. Thus, the revised version of Hadopi Law provides that Hadopi Authority could issue the first two warnings to infringers in order to stop their illegal downloads but the third warning would have to be issued by a judge, so as the right to a fair trial and to the principle of the presumption of innocence are preserved. Only after a judicial order, may the suspension of Internet access take place. At the end of 2010, the Hadopi Authority had sent 70000 recommendations by email to internet users. According to the French Law n° 2011 264 (of 11-03-2011), data collected by Hadopi are automatically transmitted to the judicial authorities in case of a request of a request and preserved during one year.

#### ***b) Digital Economy Act-UK***

The Digital Economy Act 2010 is in force in U.K. as of 12-06-2010, facing though an uncertain future. It has adopted a graduated response scheme reaching to disconnecting Internet accounts used for persistent copyright infringement. It is worth noting that Britain's two largest ISPs, in order to decide whether the Act conflicts with existing EU legislation, have sought for a judicial review of the Act on the grounds of having the potential to harm citizens and impact businesses also claiming that its provisions are not proportionate and do not respect privacy law nor comply with EU law on ISP liability. The High Court of Justice granted

---

57. Decreasing Copyright Enforcement Costs. The scope of graduated response, Olivier Bomsel & Heritiana Ranaivoson, Review of Economic Research on Copyright Issues, 2009, vol. 6 (2), pp. 13-29.

58. Law No 2009-669 of June 12, 2009, amended September 15, 2009, Journal Officiel de la Republique Francaise (J.O.), <http://www.assemblee-nationale.fr/13/pdf/ta/ta0332.pdf>.

the review permission on November 2010 and now the DEA is to be the subject of judicial review and a parliamentary inquiry.

The main grounds of ISPs application for judicial review focus on 1) UK Government's failure to give the European Commission sufficient notice for proper scrutiny of legislation, 2) non compliance of Digital Economy Act with existing EU legislation on data protection and privacy, 3) Digital Economy ACT's incompatibility with existing EU e-commerce legislation 4) disproportionality of DEA regarding their impact on ISPs business and consumers. The judge after a long hearing at London's High Court, granted permission for the judicial review on each of the four legal grounds aforementioned.

The ISPs confidence regarding a positive outcome on the judicial review is coupled with their attempt to keep the proceedings running in order to exert legal pressure in addition to political pressure on the Government to change its approach. The verdict of the High Court may take up to eight weeks while an appeal from the losing part is extremely likely as well as a possible referral to the European Court of Justice. Thus, it is still unclear whether the anti-piracy measures will be in place.

### ***c) Sinde Law-Spain***

Having one of the highest rates of illegal file-sharing in Europe, Spanish Government finally passed regulation (Sinde law), intending to reduce such high levels of illegal file sharing. Unlike France and UK, the Spanish regime includes a fast-track system for closing "unlawful" websites quickly, after a relevant judicial order, as well as the creation of an Intellectual Property Commission, depending on the Ministry of Culture, being in charge of deciding which sites should be blocked or what content is infringing and ask the person responsible for the site to remove it, after securing a judge authorization.

### ***d) Copyright (New Technologies) Amendment Act 2008-New Zealand***

New Zealand's legislative approach to graduate response is the Copyright (New Technologies) Amendment Act 2008<sup>59</sup>, introducing a notice and take down regime in New Zealand, requiring from ISPs to "adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of the account with that Internet service provider of a repeat infringer". After a huge public debate, a bill establishing a three-notice regime to discourage illegal file sharing

---

59. Available at [http://www.parliament.nz/en-NZ/PB/Legislation/Bills/b/2/a/00DBHOH\\_BILL7735\\_1-Copyright-New-Technologies-Amendment-Bill.htm](http://www.parliament.nz/en-NZ/PB/Legislation/Bills/b/2/a/00DBHOH_BILL7735_1-Copyright-New-Technologies-Amendment-Bill.htm).

was passed in New Zealand Parliament on 14-4-2011<sup>60</sup>. The regime will come into effect on 1-9-2011 including ISPs sending warning notices to their customers informing them they may have infringed copyright. After receiving notification by ISPs that three warning notices have been sent to users by the ISP, copyright holders may apply to the copyright tribunal for compensation and at the same time request to a District Court for an order requiring the ISP to suspend the account holder's Internet access for up to six months.

## V. ACTA agreement

The ACTA is an ambitious legal project, launched by Japan and U.S in order to create a new international legal framework, establishing international standards on IP rights enforcement. ACTA aims at increasing levels of IP protection in comparison to international standards created by the TRIPS Agreement. ACTA provides for the creation of a new governing body ("ACTA Committee") outside existing international institutions (i.e WTO, WIPO, etc) to address IP enforcement. It is important to note that ACTA is using- as legal foundations- existing international agreements such as TRIPS, trying to address all IP issues that are not covered up to now by TRIPS. ACTA, after its official signing, will constitute the new international standard for intellectual property enforcement. ACTA is based on 3 fundamental pillars, (a) international cooperation, (b) enforcement practices and (c) legal framework for enforcement of IP rights.

ACTA focuses on civil and digital enforcement, border measures and criminal enforcement of IP law on international level. ACTA in its latest released version does not urge participants to introduce mandatory graduated response regimes nor requires disconnection for repeat infringers and more important, omits to refer to any notice and takedown mechanism, only outlining the need of cooperation between right holders and ISPs, in order to address relevant infringements in the digital environment.

In contrast to TRIPS, ACTA contains digital enforcement provisions. Nevertheless, the final draft<sup>61</sup> does not introduce any notice and take down regime, it only stresses out the need to take "effective action against an act of infringement (...), including expeditious remedies to prevent infringement (...)"<sup>62</sup>. It also goes further requiring "endeavour to promote cooperative efforts within the business community to effectively address trademark and copyright or related rights in-

---

60. Available at [http://www.parliament.nz/en-NZ/PB/Legislation/SOPs/4/lb/49DBHOH\\_SO-P1380\\_1-Copyright-Infringing-File-Sharing-Amendment-Bill.htm](http://www.parliament.nz/en-NZ/PB/Legislation/SOPs/4/lb/49DBHOH_SO-P1380_1-Copyright-Infringing-File-Sharing-Amendment-Bill.htm).

61. ACTA - December 3, 2010, available at [http://www.ustr.gov/webfm\\_send/2417](http://www.ustr.gov/webfm_send/2417).

62. ACTA, Section 5, Art. 27.1.

fringement<sup>63</sup>”, which refers to private initiatives between ISPs and users, based on US and Ireland examples. However, the implementation of such private graduated response regimes within EU seems legally risky, since the condition of compliance with fundamental EU law principles such as freedom of expression, fair process, and privacy, may be jeopardized. In addition to the above, ACTA provides for the possibility of countries to permit competent state authorities to “order an online service provider to disclose expeditiously to a right holder information sufficient to identify a subscriber whose account was allegedly used for infringement, where that right holder has filed a legally sufficient claim of trademark or copyright or related rights infringement, and where such information is being sought for the purpose of protecting or enforcing those rights<sup>64</sup>”. A thorough look at the previous ACTA drafts proves that EU pressures led to the inclusion of specific safeguards regarding the enforcement procedure, relating to freedom of expression, fair process, and privacy.

## Conclusion

One of the main international priorities regarding IP enforcement remains the adoption of more efficient enforcement regimes either public or private, mandating a more active role for ISPs. ACTA preamble evidences the need for cooperation between right holders and ISPs, in order to address relevant infringements in the digital environment. Although ACTA does not impose a mandatory international graduated response mechanism, it expressly supports the implementation of private, voluntary graduated response mechanisms in countries where such mandatory systems do not exist, the US and Ireland serving as adequate and efficient examples of private implementation of graduated response regimes. It must be outlined though that advanced technological solutions required to address copyright infringements entail costly investments which seem doubtful during an international recession period.

Thus, the real danger that ACTA represents is the constant global pressure on policymaking towards the establishment of voluntary graduated response regimes worldwide, which may render the principle of network neutrality inactive and possibly hinder fundamental principles such as the freedom of expression and the right to privacy. The above regimes will have an explicit and direct impact on SNS as well, making it extremely controversial, if not unfeasible, to strike the balance between copyright interests and the fundamental human rights of privacy, freedom of expression and the right to a fair trial.

---

63. ACTA, Section 5, Art. 27.3.

64. ACTA, Section 5, Art. 27.4.

# **E-ID card & data protection: a path for good governance – a field of controversy**

---

**Athina Antoniou & Lilian Mitrou**

---

## **e-ID cards as a tool for e-government**

A citizen's e-ID card is used as token for identification and authentication purposes<sup>1</sup>. An e-ID card is basically a smartcard, which mostly consists of a visible field with personal information (such as the holder's name, date of birth, address, the card's issuance and expire date e.t.c) and a micro-chip, with - usually - additional personal information, which are used as holder's identifiers and are readable via a card reader device. The communication between a card and an application usually takes place via a card reader using either electrical contacts or a contactless radio frequency (RF) interface (ENISA, 2010). For the establishment of qualitative e-services, the micro-chip of an e-ID card can also incorporate digital certificates for digital signing and digital authentication of the legitimate holder, which enable or facilitate secure, yet feasible, e – transactions<sup>2</sup>.

In addition to providing services on line, the issuance of citizen's e-ID card contributes to the implementation of initiatives that aim at improving e-democracy, such as consultation or e-voting on local or even on national level<sup>3</sup>. Moreover, by issuing e-ID cards as multi-functional identification tools, the relationship be-

- 
1. According to ENISA, cards were issued in ten European (10) countries: Austria, Belgium, Estonia, Finland, Italy, the Netherlands, Portugal, Spain, Sweden and partially in UK. Germany has also issued e-ID card (started on 1 November 2010). See ENISA, Position Paper 2009, Privacy Features of European eID card specifications.
  2. The Spanish e-ID card incorporates digital certificates for digital authentication and digital signing but the interesting part is that although the latter is the token for the holder's identity, the commitment of the holder is obtained through the use of a third certificate, the content commitment certificate. See also A. Heichlinger & P. Gallego, A new e-ID card and online authentication in Spain, 2009.
  3. Estonia was the first country introducing e-voting in local elections in 2004 and in 2007 for the parliamentary elections as well. For e- voting initiatives and applications in Estonia see A. Trechsel (coordinator), "Internet Voting in the March 2007 Parliamentary Elections in Estonia" ( Report for the Council of Europe ), Epp Maaten "Towards remote e-voting: Estonian case" (2004), A Prosser and R. Krimmer ( Eds.) "Electronic Voting in Europe, Technology, Laws, Politics and Society" (2004).

tween the state and its citizens becomes de- personalized and consequently the administrative action more transparent and accountable.

Due to their main functionality as identification tools and their qualitative standards (such as the use of biometric features as identifiers), e-ID cards enable more efficient border control and the processing of relevant information. In this context e-ID cards are also used for tackling social and political challenges such as illegal immigration, illegal working, forgery and terrorism.

## e-IDs and Biometrics

E-IDs are often been conceived, designed and implemented in strict correlation with the use of biometrics. By using the term biometrics we refer to measurable biological (physiological)<sup>4</sup> features of the person that can be used for her automatic recognition as well as to the methods used for recognizing a person, based on these characteristics (National Science and Technology Commission, 2006). The use of an e-ID card, which includes biometric features as identifiers, offers more accurate identification and more secure authentication of the legitimate holder of the card, since it is based not on something that the holder knows – like a PIN number – or on something what he happens to possess – e.g. a card document – but on what she actually is (Clark, 2001). Therefore, these features can never be forgotten or lost and they are the only identifiers that can permit “negative authentication”, hence an –almost - absolute proof that a person is not who she says she is, even if she possesses a document, which proves otherwise.

Not all physiology features are suitable as an identifier, since they have to fulfill specific requirements<sup>5</sup>. The most common biometric feature used is fingertips. Digital face recognition is also used, but the most accurate and suitable in our case is eye iris (iris scan). What needs to be clarified is that it is not the biometric feature itself the one stored and processed but a template of it, hence a processed form of the biometric which holds only a part of the biometric information (FIDIS, 2007).

---

4. In the case of an e-ID card behavioral biometric are not suitable since they are not immutable in time and therefore, when we refer to biometrics as identifiers of the holder of an e-ID card, we always refer to features of her physiology.

5. According to Article 29 Data Protection Working Party “Each biometric, whether for authentication/verification or identification, is, more or less, depending on the concerned biometric: a) universal: the biometric element exists in all persons - b) unique: the biometric element must be distinctive to each person- and c) permanent: the property of the biometric element remains permanent over time for each person”. See Working Document on Biometrics, 2003.



## e-ID cards and the holder's right to informational privacy

A major concern regarding the introduction of e-ID cards refers to their wide or even enormous information value and processing potential and consequently their interference in the right to privacy and the right of informational self-determination. The question we have to deal with is if e-ID cards do represent *per se* an actual interference in the holder's rights or if their processing and – respectively – risk potential depends on the nature and use of identifiers.

Issuing e-ID cards that include unique identifiers enables and encourages wide interconnection and linkability of files and data. Although the access to specific information and the use of it may be justifiable and lawful in some cases, the indiscriminate and uncontrollable access to the person's data leads to the so-called “*function creep*” (Taylor et al, 2009), the multiple use of data for purposes beyond the ones under which their collection and processing was originally justified. This purpose alienation infringes the person's right to privacy and violates a fundamental principle of data protection regulation, the principle of finality<sup>6</sup>. This threat becomes more imminent if the e-ID card is being used as a single unique token of the citizen towards her interaction with public bodies.

The risk of “*profiling*” is also a matter of concern. By using a unique identifier for all governmental databases, which are kept separately for various – yet specified- purposes, further information about the individual can be aggregated and revealed, despite the fact that the person is principally entitled to decide, if and to which extent she decides to reveal personal information, while participating in separated aspects of public life. The collection of dispersed information in order to build the holder's “profile” and classify her in a specific group of citizens, based on criteria such as income, health condition, even family status could lead to the so-called “social sorting” (Taylor et al., 2009).

There are three options of where these data can be stored: a) in a central database, b) in the memory of a card reader, c) in the e-ID card itself, more specifically in the microchip incorporated in the card. The decision about which is the most suitable option is one of great importance, since, in practice, it is a decision of who will have legitimate access to the stored data. The major concern is, whether or not the e-ID card data will be stored in a place apart from the control of the citizen-data subject and, even more, in a central database. Storing data

---

6. The principle of finality is embedded both in the Data Protection Directive (Art. 7) and in the Charter of Fundamental Rights and Freedoms of the EU. According to Art. 8 of the Charter “Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law...”.

centrally instead of storing them in the card's microchip jeopardizes the citizens' right to privacy, mainly because it creates "*data deposits*", which can be prone to malicious practices. Besides, keeping such a database raises a lot of questions about whether the state will comply with the provisions concerning the fair and lawful use of data at any case or, at some point, will take advantage of this powerful deposit of information without the holders' knowledge (Stalder and Lyon, 2009).

### **Biometric vs. Informational Privacy?**

The use of biometrics as unique identifiers might even introduce more security risks than it aims to reduce. Their use is widely associated with criminal activities and investigation of crime by police and judicial authorities. Irrespective of the moral issue of "incriminating" citizens – holders of e-ID cards, the collection and storage of the holder's biometrics is founded strictly on identification and authentication purposes, therefore any potential use as incriminating evidents against the holder leads to a profound inconsistency with the legal system restricting the fundamental principle of a person's right against self-incrimination and the principle of proportionality. The collection of such elements could be justifiable only at hoc and always in compliance with the relevant legal requirements. Taking into consideration that biometrics are, in fact, features of our physiology and acknowledged as the holder's personal the use of a person's personal data for the same person's incrimination is not without concern, especially in countries where holding such an e-ID card is mandatory (FIDIS, 2009).

Another major concern refers to the acknowledgement that despite the high level of accuracy, biometrics can lie. It is highly more difficult than usual but the possibility of a false enrollment, a false match or a wrong management of the method is still real and reduces the alleged advantage of using biometrics (Clark, 2001, Liberatore, 2005). The case of a lawyer from Oregon, who was falsely accused of being implicated in a deadly train bombing in Madrid and was jailed for two weeks (de Hert, 2005) is a livid proof that errors can actually occur and when they do, legal rights are at risk. In that case, taking into account that the issuance of an e-ID card with biometric features creates a permanent bond between the holder and the card, a person must prove that she is not who her own physiology feature say she is. This complicates the lawful operation of the legal system since it leads to untrustworthy results, but the most important is that it makes it extremely difficult for the person to exercise her legal rights.

Furthermore, considering that there are types of biometrics that can be collecting even without our knowledge (e.g. fingertips we leave in things we use) if the biometrical template is stored in a central database and the alleged owner has

absolutely no control over its use, a technical error, a successful hacker- attack or just a wrong management of the central database exposes millions of people to threats of vital importance for their legal rights. In addition, the indiscriminate and proactive collection of fingerprints of law-abiding citizens is perhaps not the politically correct way to establish trust between the state and the citizens and could lead to a wide “*trust gap*” among them, although citizens’ trust is actually a *conditio “sine qua non”* for the acceptance of e-ID cards by citizens.

### **e-ID cards: is there a rights-preserving solution?**

The fundamental legal basis of processing personal data is abiding by the principle of finality, i.e. processing data for specified, explicit and legitimate purposes (FIDIS, 2007). The data of a holder of an e-ID card must not be processed further in a way incompatible with the purpose for which they were initially collected and processed. The requirement for the specification of the purpose excludes principally merging or interconnecting databases, which are kept for different purposes or collecting and using data for vague purposes e.g. for public interest in general with no specified purposes. In addition, the purposes for processing personal data must be known to the individuals *ex ante* and not after the processing. That means that a proactive collection and storage of data does not comply with the requirements deriving from the principle of finality. Considering that an e-ID card, used as a unique identifier, is in fact a multi – functional identifier with many purposes to serve, the requirement for *ex ante* specific and explicit purposes is hardly adjustable in that case. Furthermore, if the holders’ personal data are stored in central databases a huge amount of personal information can easily be used for multiple, irrelevant and, even, illegal purposes without the person’s knowledge.

All these requirements can be addressed by using different identifiers for different sectors instead of a unique identifier. Issuing an e-ID card as a unique identifier of the citizen, used in all his transactions with governmental bodies turns it into a unique “*access key*” in scattered databases. Due to the fact that multiple identifiers are used for specific applications, wider interconnection of data can be prevented and the balance between privacy and the introduction of a functional e-ID card can be addressed. Domain-specific identifiers can be derived from (secret) identifiers held by a trusted central issuer.

The Austrian E-Government Act<sup>7</sup> is a very interesting framework, a benchmark of introducing such domain-specific identifiers. The person’s identification in dif-

---

7. The Austrian E-Government Act, Federal Act on Provisions Facilitating Electronic Communications with Public Bodies, Art. 1 of the Act published in the Austrian Federal Law Gazette,

ferent public bodies is based on different identifiers with limited use, created by encrypting the source PIN which uniquely identifies the holder in the card but is not the one transmitted to the communication partner. The fact that the Data Protection Authority is the one in charge of encrypting the identifiers as the trusted central issuer enhances public trust and associates identity management with data protection.

Another substantive pillar for protecting privacy is the principle of proportionality. This principle is proved to be of vital importance for the evaluation and balance of public interest and the holder's right to informational privacy. In the case of an e-ID card, the stored and processed data not only should be in compliance with the requirement for specified, explicit and legitimate purposes but there has to be a legally accepted balance between the means and the purpose which the means serve as well.

The requirement to address proportionality becomes even more crucial in the case of e-ID cards with biometrics features. In order to reveal only the minimum information required for serving the legitimate purposes it is not the biometric feature itself that should be stored but a template of it, which must be further encrypted in order to safeguard that no health data or any other personal information can be revealed or cross checked so as to reveal additional information about the e-ID holder. Nevertheless, irrespective of the template storage, biometrics can only be used where no other means of identification or authentication is appropriate but even then, the less privacy – pervasive method must be chosen<sup>8</sup> and they should never be used alone.

It should also be noted that when the micro-chip of an e-ID card incorporates a certificate for digital authentication and another one for digital signing, a digital signature should not be required for authentication purposes, since this is a non – proportional measure for achieving the purpose of authenticating for a public service. This is based on the grounds that digital signature leaves irrevocable traces beyond the actual fact of authentication and reveals information beyond the minimum required, hence such a practice must be avoided.

The risk of storing inaccurate or incomplete data and attribute them to the citizens is another risk. In order to avoid false enrolments and keep reliable, up-dated information about the holders the introduction of e-Ids or at least the security and privacy policy has to be reviewed on a regular basis. Public bodies responsi-

---

part I, Nr. 10/2004, entered into force on 1 March 2004.

8. On this ground the French Data Protection Commission (CNIL) has refused the use of fingerprints in the case of access by children to a school restaurant, but accepted for the same purpose the use of the outline of the hand pattern.

ble for the maintenance of the respective databases have to re-examine the necessity to keep data in a form which permits the identification of data subjects and restore any inconsistency between the necessary time of storage and the actual time of storage. The latest requirement is not easily applicable taking into account that e-ID card constitutes a token, used in many legally bounded and binding transactions between the holder and the state.

Collecting and processing e-ID holders' personal data must be grounded on at least one of the legal basis of processing. The primate legal basis is the person's consent but it is highly questionable if due to the imbalance of power between the citizen and the public authorities, the consent can be given freely<sup>9</sup>. Article 7 e of the Data Protection Directive provides for the lawfulness of personal data processing if it is required for the performance of a task carried out in the public interest of in the exercise of official authority vested in the controller or to a third party, to whom the data are disclosed. This seems to be an applicable legal basis in the case of issuing an e-ID card, especially when this issuance is mandatory for citizens. In addition, according to Article 7 f of the Data Protection Directive, processing of personal data is legitimate if it is necessary for the purposes of the legitimate interests pursued by the controller of the third party or the parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject, in our case the holder of an e-ID card. In our opinion however, both the collection and further processing with regard to e-Ids and the access to the information included must should laid down by a specific law, which should include detailed provisions concerning the authorities entitled to access and use of information as well as the procedures and the institutional guarantees of the citizens' rights such as the competences of the data protection authority and the information and access rights of the e-ID holders<sup>10</sup>. The bodies and institutions with access rights, the specific data they are allowed to access and the purposes, on which they establish their access rights must be explicitly determined. A precise determination of who – when and why gains access to the holder's data is a essential factor for enhancing databases security and safeguarding the holder's right to privacy.

### The Greek case

The Greek government has announced the introduction of e-ID cards in order to promote secure e-government services and reduce administrative burdens.

9. Article 29 Data Protection Working Party, "The future of privacy", p.17.

10. According to the Charter of Fundamental Rights (article 8) and the 95/46 EU Directive (article 7).

Greece's legal framework is till now based on the use of multiple identifiers, such as the citizen's social security number (AMKA), the number of the traditional ID card (ΑΔΤ) and a number for tax registration (ΑΦΜ). Even before the amendment of 2001, where the right to data protection was expressly embedded in the Greek Constitution, the general principle of respect and protection of the value of the human being (Art 2 par. 1), the persons' right to develop freely their personality (Art. 5 par. 1) and – actually less! – the person's right to protect private and family life (Art. 9) offered already the constitutional basis for privacy and data protection. The use of a unique identifier is regarded as incompatible with these fundamental rights (Drogkaris et. al, 2008), as it equates the individual with a "number". The use of a unique identifier allows principally the aggregation of information, which is available in the public sector and the profiling of the citizen<sup>11</sup>. Moreover we should not underestimate the risk of use of personal information either by authorities for a variety of purposes not approved by the citizen or laid down by law or the risk of misuse by civil servants for private and thus unlawful purposes.

Furthermore, the so-called interconnection of files and databases is explicitly regulated in the Greek Data Protection Law (Act 2472/97). The Greek regulator regarded the use of common identifiers as an potential infringement of the persons' right to informational privacy and therefore the Law sets specific institutional requirements, providing that any interconnection of files and databases must be communicated to the Data Protection Authority and if one or more of the "linked" files/databases contains sensitive data (or if the interconnection results in the disclosure of any sensitive data) or if a "uniform code number" is to be used as means for the interconnection, a permit must be issued by the Authority<sup>12</sup>.

Taking into account that the issuance of a unique identifier in the citizens' Greek e-ID card contravenes the relevant legal framework, that is the above mentioned fundamental principles and constitutional rights of the data subjects an affordable solution could be the use of the so-called sector – specific identifiers under the specific privacy requirements mentioned above.

---

11. That is why although the issuance of a unique code number as a unique identifier was introduced in 1986, this provision was never actually implemented and it was abolished in 1991.

12. According to Act 2472/97, Article 8 par.3 *"If at least one of the files about to be interconnected contains sensitive data or if the interconnection results to the disclosure of sensitive data or if for the implementation of the interconnection a uniform code number is to be used, such an interconnection will be permitted only following a prior permit by the Authority (interconnection permit)".*

## Concluding remarks

The answer on whether the issuance of citizens' e-ID cards can be in compliance with the person's right to privacy and data protection is neither negative, nor positive ex ante. Actually the answer depends on the framework we choose to implement and on the means we choose for its application as well as on the procedures and guarantees in place to ensure the respect of the rights of the citizens. The use of multiple, domain-specific identifiers as e-ID cards' privacy features, the demand for strict application of the principle of proportionality against wide collection of data in addition to the requirement for specification of the purposes on a solid and accessible to citizens legal ground can be considered as key - factors in order to address the privacy risks emerging from the issuance of e-ID cards.

## References

ARTICLE 29 Data Protection Working Party (Working Party on Police and Justice), 2009. Working Paper "The Future of Privacy, Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data".

Beynon-Davies P., (2004). "EBMS Working Paper EBMS/2004/2 Personal Identification in the Information Age: The Case of the National Identity Card in the UK", European Business Management School

Clarke R., "Biometrics and Privacy" <http://www.rogerclarke.com/DV/Biometrics.html>

Drogkaris P., Geneiatakis D., Gritzalis S., Lambrinoudakis K. and Mitrou L., (2008). Towards an Enhanced Authentication Framework for E Government Services: The Greek Case, Proceedings of the EGOV' 08 -7<sup>th</sup> International Conference on Electronic Government, Torino September 2008, Trauner Verlag pp. 189-196.

ENISA (2009). "Privacy features of European e ID Card Specifications", Position Paper

FIDIS (2005). (Future of Identity in the Information Society) "D3.16: Biometrics: PET or PIT?"

Heichlinger A. & Gallego P., (2010). A new e-ID card and online authentication in Spain, published with open access at Springerlink.com

Hert P., (2005). "Biometrics: Legal Issues and implications", Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission

Liberatore A., (2005). *"Balancing Security and Democracy, The Politics of Biometric Identifications in the European Union"*, European University Institute, Robert Schuman Centre for Advanced Studies, EUI Working Papers RSCAS No2005/30

Lyon D., (2009). *"Identifying Citizens, ID Cards as Surveillance"*,.....

Lyon D., (2007). *"National ID Cards: Crime – Control, Citizenship and Social Sorting"*, article published by Oxford University Press

Prosser, Krimmer (2004). *"Electronic Voting in Europe, Technology, Laws, Politics and Society"*

Maaten Epp (2004). *"Towards remote e-voting: Estonian case"*, Workshop of the ESF TED Programme together with GI and OCG

SK, (2003). *"The Estonian ID Card and Digital Signature Concept, Principles and Solutions"* (White Paper Version June

Felix Stalder F. and David Lyon D., (2009). *"Electronic Identity Cards and Social Classification"* in *"Surveillance as social sorting, Privacy and Digital Discrimination"*

Taylor J. –Lips M. –Organ J., (2009). *"Identification practices in government: citizen surveillance and the quest for public service improvement"*, article, Identity Journal Limited

Trechsel A. (coordinator), (2007). *"Internet Voting in the March 2007 Parliamentary Elections in Estonia"*, European University Institute, Robert Schuman Centre for Advanced Studies, Report for the Council of Europe



# **The European Commission's policy on the harmonization of protection of the moral rights of authors and performers in the European Union**

---

---

**Theodore Asprogerakas – Grivas**

---

---

Harmonization of national laws is a fundamental obligation for the European Commission. The very foundations of the Union were based on the common intention of the Member States to harmonise to the maximum possible extent the Internal Market.

In the past 25 years, the Commission has made constant and significant efforts to harmonise the national laws of the Member States in the field of intellectual property rights. Many Directives directly related to copyright are now in force while many others related to other intellectual property also subsist. Legislation here is more extensive than in any other field of harmonization.

One should normally expect that moral rights' harmonization would be part of the general harmonization efforts of copyright and related rights.

However, the European Commission has so far made no attempt to harmonise intellectual property in the field of moral rights. This is a rather surprising fact considering that in the last twenty five years EC has made tremendous efforts on harmonising the economic rights of authors and beneficiaries of related rights by issuing many Directives, including term and enforcement of protection<sup>1</sup>. Moreover, EC is very keen on bringing actions before the European Court of Justice

---

1. Namely, the following Directives: a) Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, b) Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the protection of databases, c) Council Directive 91/250/EEC of 14 May 1991 on the protection of computer programs, d) Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, e) Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art, f) Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, g) Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (codified version) and f)

against any Member State failing to embody correctly or fully comply with the requirements of the above mentioned Directives and introducing exceptions and limitations. Many terms of the above mentioned Directives have been an object of analysis and definition by the European Court of Justice.

On the other hand, no official instrument has been issued in harmonising the field of moral rights of same beneficiaries (authors and holders of neighbouring rights).

One should first discuss the past of moral rights' harmonization attempts, within the EU.

The issue of harmonization of Union laws was under examination since the year 1988, when addressed by Commission's 1988 "Green Paper – Copyright and the Challenge for Technology"<sup>2, 3</sup>.

Moral rights protection was also among the points listed in the Commission's «Follow-up to the Green Paper- Working Programme of the Commission in the Field of Copyright and Neighbouring Rights" under chapter 8.3 in 1991<sup>4</sup>. Hearings of all interested parties were held on 30.11 and 1.12.1992. The beneficiaries of protection aimed to strong moral rights, while the entrepreneurs were opposed to such protection.

The "Green Paper - Copyright and Related Rights in the Information Society"<sup>5</sup> addressed the issue of moral rights' harmonization under section VII of Part 2 but only in order to carry the process of consultation further<sup>6</sup>.

The 1996's "Follow-up to the Green Paper - Copyright and related rights in the information society"<sup>7</sup> addressed again the issue of moral rights and the impact of the different moral rights national regimes in the common market under chapter 4. However, the only proposed action was the conduct of a further study on the

---

Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection and certain related rights (codified version).

2. COM(88)172 final, June 1988.

3. C. Seville, *EU Intellectual Property Law and Policy* (Edward Elgar, 2009), par.2.3.1.

4. COM(90)584 final, 17.1.1991.

5. COM(95)382 final, 19.7.1995.

6. See also T. Hoeren, "The Green Paper on Copyright and Related Rights in the Information Society" (1995) 17(10) *E.I.P.R.* 511-514.

7. COM (96) 568 final, 20.11.1996.

issue. The issue of harmonization of moral rights' protection started to weaken and the opinions supporting such harmonization were scarce<sup>8</sup>.

The 2004's "Commission Staff Working Paper on the review of the EC legal framework on the field of copyright and related rights"<sup>9</sup> considered that under par.3.5, there was no evidence that moral rights' current state affected the good functioning of the internal market in the digital environment, and thus, concluded that no harmonization was necessary.

The recent 2008 Green Paper on Copyright in the Knowledge Economy<sup>10</sup> makes absolutely no reference to the moral rights of authors and performers. Moral rights are officially no longer on the Commission's agenda.<sup>11</sup>

In addition, the satellite and cable<sup>12</sup> in rec.28, the Database Directive<sup>13</sup> in rec.28, the Copyright Directive<sup>14</sup> in rec.19 and the Term Directive (codified version)<sup>15</sup> in rec.20 and art.9 explicitly state that their respective provisions do not affect moral rights.

It is therefore objectively clear that the Commission is reluctant to proceed with such harmonization. The questions arising are numerous and significant: Is such reluctance justified? Why has the Commission not yet attempted to harmonise authors' and performers' moral rights?

As there is no official response from the Commission on this issue, an argumentation for the Commission's reluctance to proceed to the harmonization of moral rights will be attempted.

One argument could be that the Member States themselves neither require nor favour moral rights harmonization. A study of M. Salokannel, A. Strowel and E. Derclaye published on April 2000 under a study contract<sup>16</sup> with the EC con-

---

8. See par.5.2.8 of the Opinion of the Economic and Social Committee on the "Green Paper - Copyright and Related Rights in the Information Society".

9. SEC (2004) 995, 19.7.2004.

10. COM (2008) 466 final, 16.7.2008.

11. See further Kallinikou, D. *Pneumatiki idioktisia & syggenika dikaionomata* (Sakkoulas, 2008), p. 525 (in Greek).

12. OJ [1993] L248, p.0015-0021.

13. OJ [1996] L077, p.0020-0028.

14. OJ [2001] L167, p.0010-0019.

15. OJ [2006] L372, p.0012-0018.

16. Study contract ETD/99/B5-3000/E28 commissioned by DG Internal Market.

cludes, among others, that governments saw a need for the harmonising moral rights except those of Italy and Greece.

However, one could counter argue against this view.

Firstly, EC did not accept the conclusions of this study, at least officially. A statement attached to the study clearly states that European Commission is not whatsoever bound by this study.

Secondly, the European Commission neither needs nor requires a Member State's consensus in order to proceed with a harmonization program. Its harmonization authority comes directly from the EC Treaty and no consensus prerequisites exist. Articles 94 & 95 of the EC Treaty oblige the Commission to harmonise the domestic legislatures in order to establish a common market to all aspects; there is no reason why moral rights should be excluded. Furthermore, in only few cases the European Commission asked for a consensus or opened public dialogues with the Member States before the Council proceeds to legislation.

A third fact that should be mentioned is that, nowadays European Union is much expanded with the addition of ten new Member States. The year's 2000 study does not reflect the current situation.

Another argument could be that the moral rights of authors and performers are already harmonised by the Berne Convention, the WIPO Copyright Treaty, 1996 (WCT) and the WIPO Performances and Phonograms Treaty 1996 (WPPT), which have been ratified by all Member States. Recital 19 of the Copyright Directive's Preamble clearly adopts this argument. This could be considered as an official opinion of the European Commission.

However, this opinion would also leave significant gaps: The three Treaties harmonise only a limited number of moral rights to a limited number of beneficiaries, while the Treaties do not contain any provisions in the fields of exceptions, limitations and exercise of moral rights. Moreover, the WPPT protects the moral rights of the performers of aural performances or performances fixed in phonograms only, leaving all other performers and performances out of the scope of its protection<sup>17</sup>.

Under this view, it seems that harmonization made by the above international instruments is limited and therefore insufficient.

---

17. Ricketson S. and Ginsburg J., *International copyright and neighbouring rights* (OUP, 2006), vol. ii, par.19.53 (ii). For a comparison of moral rights in the EU and the US see Spinello & Bottis, *A defense of Intellectual property Rights*, 2009, pp. 81, 98, 99.

Another argument for the non harmonization of moral rights could be the fear of the Member States that such harmonization at an EU level could possibly lead to lowering the level of protection. However, this argument is not very persuasive. Harmonization has usually led to an increase protection, when it comes to intellectual property rights. Moreover, if this fear was justified, the common law countries, which traditionally aimed for a minimum (if not none at all) protection of moral rights would favour and lobbying for such harmonization, which they apparently do not.

A harmonization effort, that is not broadly known, was tried by the Social Commission during the preparation of a Directive amending and codifying the Term Directive<sup>18</sup>. However, European Commission considered that the strengthening of moral rights has no financial impact on performers and record producers, and thus, would not make an incremental contribution to performers' remuneration<sup>19</sup>. Moreover, that the strengthening and harmonising the moral rights of performers, would bring some non-pecuniary benefits to performers, by allowing them to restrict objectionable uses of their performances<sup>20</sup>.

However, strong counter argumentation can be put forward. The significant differences between the various moral rights regimes not only reduce the remuneration of authors and performers but, at the same time, affect severely the common market. That was also one of the conclusions of the 2000 aforementioned study of the Commission<sup>21</sup>.

An obvious example is the works made by employees, where in the common law countries the authors-employees enjoy no moral rights protection, while in the continental countries they enjoy full protection of their moral rights and can object to certain uses. An extensive number of fair dealing uses can nullify the moral right protection of authors and performers in UK, while in many continental countries such exceptions do not even exist. Similar situations arise in works of collaboration, or collective works, while the exploitation of a work in transformative ways in the internet would be subject to completely different treatment from one Member State to another concerning the moral rights different regimes.<sup>22</sup> Needless to add, that authors could exercise their moral right of access or retract to some Member States, while in others not. Generally speaking,

---

18. OJ [1993] L 290, p.0009.

19. See COM (2008) 464 final proposal of 17.7.2008.

20. The EC's proposal was admitted and rec.20 of Directive 2006/116 clarifies that it does not apply to moral rights.

21. However, the 2004 Working Paper concludes to the opposite conclusion.

22. See Makeen M.F., *Copyright in a global information Society* (Kluwer, 2000), p. 281-284.

authors and performers relying on their moral rights protection regimes can object to certain exploitation uses of their works or performances in some Member States, while for the same uses they cannot in others. Therefore, the impact on the internal market is severe.

Given the above evaluation, it is submitted that the reluctance of the European Commission to proceed with the harmonization of the moral rights of authors and performers within the internal market is not fully justified.

On the other hand, they seem to be many reasons which would justify such harmonization on EU level. As mentioned before, the internal market will be harmonised, thus an accomplishment of extreme significance would be achieved by EC. Harmonization of the internal market is an obligation and not a right for EC; therefore, EC has to act where need of harmonization occurs. Moral rights are a field where such harmonization is required.

Another argument favouring harmonization is the avoidance of discrimination, which arises by the different treatment of performers' moral rights protection. Specifically, performers of works of sound have their fundamental paternity and integrity rights secured, while other performers (for example actors, dancers) do not. This clearly is a discrimination which seems difficult to justify under arts. 12 & 13 of the EC Treaty.<sup>23</sup>

The same situation arises also for the moral rights of authors to the extent that authors of continental countries enjoy a significantly wider range of moral rights protection (including to their subject matter the rights of divulgation, access and retraction) than in others. The result is the same as above, namely an arguably unjustifiable discrimination.

Moreover, in the majority of the national intellectual property laws of the EC Member States, the moral rights and the economic rights of a work or a performance are the two sides of the same coin, under either the monistic or the dualistic view. It is only to the common law countries, where copyright is completely separated from the moral rights. Under these circumstances, it could hardly be justified how it is possible for EC to harmonise one side of the coin (economic rights of authors and performers) and not the other (their respective moral rights).

Furthermore, one should consider the cultural protection<sup>24</sup>. It is generally accepted that moral rights by their very nature represent the bond between the author (or the performer) and his creation (or his performance respectively). The law of

---

23. See par.33 of the Opinion of Advocate General in case C-360/00 P *Land Hessen v G. Ricordi & Co. Bühnen- und Musikverlag GmbH* [2002] ECR I-5089.

24. EC Treaty (Amsterdam) art.151.

intellectual property should be able to promote cultural growth and protection. It would also be beneficial for cultural diversity<sup>25</sup>. The moral rights regime is a strong weapon in the hands of authors and performers, which protects them from the abuse of their rights and safeguards them from abolishing any bond with their respective works and performances when the economic rights are assigned (or pass with any reason) to another person or legal body. This protection guarantees support and reward for the creative activity and the benefit of progress of authors and performers. Therefore, EC is justified to proceed with such harmonization, based on its obligation to protect and promote cultural inheritance in Europe.

On the other hand, cultural protection and moral rights are two different things. No one can argue persuasively that promoting moral rights will make the intellectual property market flourish. The situation in UK proves exactly the opposite<sup>26</sup>: Weak moral rights protection and, particularly, the existence of provisions allowing the unconditional waiver and consent of moral rights of both authors and performers have led the entrepreneurs to invest more in the exploitation of the economic rights of copyrighted works. The result is that the common law countries (including UK) film and record industry is among the strongest worldwide<sup>27</sup>. Without exception, none of the continental European countries can match the growth and impact of the UK's copyright industry. One should add that authors also benefit from this situation; as long as entrepreneurs invest to the exploitation of their creations, they are motivated to create more. One could safely argue that we have already reached a time that the demand for the exploitation of new works exceeds the offer. This led in the past years to new ways of exploitation of user generated content by major internet enterprises, such as YouTube and MySpace<sup>28</sup>. This however, does not constitute a reason for totally excluding moral rights from the harmonization process.

Another serious issue that also favours further harmonization is the existing incompatibilities within the Member States' legislations against the international

---

25. Same argument was adopted under par.7.4 in Commission's staff working document accompanying the proposal for a Council directive amending Directive 2006/116/EC as regards the term of protection of copyright and related rights - impact assessment on the legal and economic situation of performers and record producers in the European Union [COM(2008)464 final].

26. See Kingston W., "Why harmonization is a trojan horse" (2004), *E.I.P.R.*, 26 (10), p. 447-460.

27. See also Kamina P., *Film copyright in the European Union*, (CUP, 2002), p. 61.

28. Also Griffiths I. and Doherty M., "The harmonization of European Union copyright law for the digital age" (2000), *E.I.P.R.*, 22 (1), p. 17-23.

instruments provisions<sup>29</sup>. A characteristic example is the requirement of assertion<sup>30</sup> of the UK's Copyright Designs & Patents Act in order for the paternity right to be exercisable. This requirement could arguably be held incompatible with the provisions of articles 5(2) and 6bis of Berne Convention. More incompatibilities are likely to exist among the different legislations of the EU Member States; the elimination of which constitutes a further argument favouring the harmonization in the field of moral rights. One should further consider that failure of full compliance with the Berne Convention's provisions can lead to an action before the ECJ<sup>31</sup>.

One could counter-argue that such harmonization does not guarantee full compatibility of legislations to the international or EU provisions. This is true. However, in this situation an action before the ECJ is very likely to be brought against the infringing nation and the matter be judged there. The process of harmonization is neither always easy nor automatic. Long transformation of domestic legislatures or litigation may be needed, but this is the only way. The non-compliant Member States will be treated accordingly.

For all the reasons analyzed above, harmonization of the regime of authors' and performers' moral rights within the EU seems legally justified.

---

29. See also Sterling J.A.L., "International codification of copyright law: possibilities and imperatives-Part 2" (2002), *I.I.C.*, 33(4), p. 464-484.

30. CDPA, ss.78 & 205.

31. See case C-13/00 *Commission of the European Communities v Republic of Ireland* [2002] 2 CMLR 10.



# **The threat to consumers' privacy: digital management systems of protection of privacy and personal data**

---

---

**Victoria Banti-Markouti**

---

---

*"On the internet nobody knows you are a dog"*  
(The Economist, 31/5/1997)

## **I. The violation of data by the technological protection measures of intellectual property works (Digital Rights Management Systems) in the internet**

The initial theory of privacy, "the right to be let alone", as it was formulated in 1890 by Warren and Brandeis, is rather general. "There is no privacy in the internet. Get over it! We have to live our lives ready to see our dirty laundry on a cover", stated Jeffry Cole (2011) one of the most well known academics of the digital environment. This very explicit comment is showing in a very provocative manner the evolution of privacy theories within the last centuries.

How is the right to privacy affected by the protection mechanisms of intellectual property in the internet? In the real world the rules of intellectual property do not require that each purchaser of a book, film or musical work will give his/her personal data each time he/she purchases a product. However, this rule is not in effect when the purchaser or user of work of intellectual property via internet is asked directly or indirectly to give his personal data so that he can enjoy the intellectual good of his choice.

In about a decade ago the article of a number of experts in the field explained very clearly the interconnection between intellectual property protection and data violations: "Our claim is simply that the use of these techniques can affect user privacy and that this fact should be taken into account at every stage of DRM-system design, development, and deployment. At the risk of stating the obvious, we note that there can be inherent tension between the copyright-enforcement goals of owners and distributors who deploy DRM systems and the privacy goals of users" (Feigenbaum et al. 2001).

Types of spyware can be easily found in products of intellectual property that are sold in electronic form. In real life when somebody buys a product of software

from the local shop of computers the contract is completed at the moment where the buyer gives the money and receives the box that contains the disk with the product. Most users in order to gain time during the installation never read the content of all windows that are presented and clicks 'yes' to all the boxes without reading their content. This process is difficult to be considered as legal since the contract and its terms have been completed in the shop with the attribution of price. Nevertheless the boxes that appear in the computer screen change *a posteriori* the terms of convention. The text that basically the users do not read even if they step the button "I agree" is binding. Therefore, the users agree to reveal their personal data so that they will enjoy a work of intellectual property in electronic form (Klang 2003).

When the English courts found themselves in front of this offence in the case *Spurling v. Bradshaw*, 1956, Lord Denning proposed that all the above terms should be presented with red letters in the package of the product so that the consumer is informed before buying. The same argument can be used for contracts on intellectual property works (Klang 2003).

Further, if the user accepts the cookies but denies giving away his personal data in digital applications and bulletins of order, for example the address, then services as purchases of work of intellectual property via internet is rendered impossible. This solution requires knowledge of informative systems so as to install and run the essential software in order to exterminate the spying software that illegally has been installed in a user's computer.

These technological measures used for copyright protection, such as the Digital Rights Management Systems, which are described in the Digital Millennium Copyright Act (DMCA) and the Information Society Directive, change substantially the degree of privacy of users of intellectual goods via internet. At the same time these mechanisms made the access of the copyright work more difficult as well as the application of the exception of copyright such as making copies for private, fair use.

The directive on the protection of personal data 95/46/EC forecasts that the subject of personal data will be supposed to give his consent for the use of his data for advertising aims. Also, it places the obligation to the member states to ensure that the citizens are informed for the particular right. The particular regulation tried to give solution in the cases of unverifiable publicity without the consent of recipients. Similar is the problem in the internet with the sending of advertising messages without the consent of recipient (spam).

The future of privacy is connected more and more with the future of the protection of copyright. The industry of intellectual property created systems of protec-

tion which allow perfect control of the access and use of digital files violating the privacy of the users. Collected information may include data about content retrieval and accessing, frequency, access locations. The purposes for collecting data may include personalized use for direct marketing backup and archives, profiling of customers, customer service and retention (Feigenbaum et al. 2001).

The technological measures of protection of intellectual property are consisted of special software in order ensure that only legal use is possible. On the other hand the controllers of personal data use the same technology so that they ensure the rights of subjects of personal data. For example disc shops offer songs in cryptographic format so that can be decoded only from concrete appliances and only if concrete keys are used. The same techniques could be also used for private information. The consumer can clarify, for example that only the controller of personal data can communicate with him via his electronic address and not any third party.

## **II. Criticism of data violations by the technological protection measures of intellectual property works**

The civil society of internet users, the political world and academia have severely criticised the above mentioned used of DRMS that violate privacy. The have also criticised the same mechanisms because they make the application of exemptions to copyright rather difficult.

Will the code replace the law? Are we heading towards a world that every use of information is being controlled automatically? Are we heading towards a pay-per-view society that DRMS are controlling and reducing the access of the public to information? How would the market be affected if the users knew that their data would be revealed automatically after buying the product? These are some of the questions of the academic world.

Daniel Solove has proposed a taxonomy of privacy to model the problems of privacy harms. His taxonomy includes among others Information Collection for surveillance, Information Processing for identification of users, Information Dissemination for breach of confidential information or blackmail, invasion for decisional interference (Solove 2007).

A characteristic example of the citizen's reaction as it is reflected in politics is the rise of the Pirates' Party in Sweden which gained 7% of the votes in the euro parliament elections of 2009. The facts that lead to its publicity were firstly the incorporation of the directive 2004/48 on the enforcement of intellectual property rights which demands that the service providers should reveal the data of the users who infringe copyright works on the internet and secondly the conviction

of the holders of Pirate Bay webpage in one year imprisonment and penalty of 2,5 million Euros. Furthermore, the German Pirate Party won ap. 1% on these elections and registered "pirate parties" exist in Austria, Denmark, Finland, Poland and Spain and groups are attempting to register as political parties in the UK and the US (Edwards 2009). This rise of the pirate parties indicates not only the growing public awareness of internet issues but also the voices for further protection through relevant legislation.

The role of the public opinion can indeed be effective to the protection of users' rights. As an example we could mention the creation of consumer protective legislation and information of consumers on their rights in the US. As a result of the public opinion's pressure the "Digital Media Consumer's Rights Act" was enforced in 2002, that is also known as "the digital consumer right to know", and obliges the manufacturers of intellectual property to inform the consumers for the digital rights managements systems and their implications.

### **III. 'The answer in the machine is the machine'- methods of consumers' control of their personal data**

Consequently, concerning the protection of personal data in the internet the phrase "the answer to the machine is the machine" was applicable. The same technology that is used for privacy invasion can be used for privacy protection. These technological mechanisms (privacy enhancing technologies) correspond to the idea of Reidenberg (1998) for Lex Informatica and to the arguments of Lessig (1999) for the lawful effects of the code of computers.

More specifically, Lessig makes an interesting comparison between different choices as for the question of privacy in the internet. He compares two from the most famous American universities, the University of Chicago and Harvard as for the methods that they use for the access in the internet. In the first university each student or employee can have access in the internet from any computer anonymously. On the contrary, in Harvard the students and the employees can enter in the internet only after registration so that all their activities in the internet can be controlled. These two practices have explicit impact in the freedom of expression, privacy and other values. This difference for Lessig is not a difference of code but a difference of software. These networks are not determined by their nature but by their architecture (Bennet 2003).

Although technology appears to have negative repercussions for the protection of personal data, it could also be used in order to improve privacy protection. More specifically, Lessig speaks for the application of the same technology aiming at the abolition of negative phenomena that the same technology creates. His idea for software as means that determines the behaviour is not new. Similar was also

the theory for *lex informatica* by Joel Reidenberg. The first example of this strategy was in 1999 when Intel Corporation announced the new generation processor Pentium III. Intel considered that it was a good idea that each instrument has its code so that the big companies can find the machines as these are moved by region to region, asset-tracking.

Since the answer to the machine is the machine new privacy enhancing technologies (PETs) were developed for the protection of data in the internet. According to the recent PETs definition by the EU Commission delegated report "PETs is a complex concept that comprises a broad range of individual technologies at different levels of maturity. PETs are constantly evolving, often in response to ever more advanced threats. Data security technologies are PETs if they are used to enhance privacy. But, it should be noted that they can be used in inherently privacy invasive application, in which case they cannot properly be counted as PETs. Data minimisation and consent mechanism are an important part of PETs. Many PETs combine various technologies, including data protection tools (e.g., encryption) and 'pure' PETs (e.g., data minimisation tools) to form integrated PET systems of varying complexity" (Study on the economic benefits of privacy- enhancing technologies (PETs) (London Economics 2010).

Similarly, the creation of The Platform for Privacy Preferences (P3P) Project, which is supported by the World Wide Web Consortium (W3C), has the aim to determine how the system will use the personal information. P3P gained ground and it appears that it will become standard that is used by a number of companies. At the same time, it is considered that provided that the users acquire comfort with this system of protection the need for legislation relative with the protection of personal data will be limited. In the initiative Platform for Privacy Preferences (P3P), which was manufactured by the Wide Web Consortium (W3C), the consumers can use browsers or other software in order to read the policy of a web page with regard to the privacy and the above tools compare automatically if the preferences of the user coincide with the policy of the particular page so that his privacy is protected as he, himself has selected (Bennet & Raad 2003). Technology P3P has been adopted also from the Microsoft Internet Browser so that the users can select between five degrees of protection. With this way before the user enters in a web page the browser communicates with the policy about privacy of that page and communicates the user if his expectations about privacy are satisfied.

In addition, the information of citizens with regard to the potential offences of their personal data at their access in work of intellectual property in the internet is very much needed. As an example we could mention the Privacy Enhancing Technologies annual Symposium in Canada which "addresses the design and real-

ization of such privacy services for the Internet and other data systems and communication networks by bringing together anonymity and privacy experts from around the world to discuss recent advances and new perspectives”.

On the other side of the Atlantic, within the EU, the PRIME project is a research project that aims to demonstrate viable solutions to privacy-enhancing identity management by delivering a reference framework, requirements, an architecture, design guidelines, protocols and prototype implementations that are evaluated from a multidisciplinary perspective. The prototypes are not intended as final products for commercial deployment.

However, there is still doubt on the affectivity of such privacy protection measures. It has been argued that they do not have up to now contributed enough in the protection of personal data. This is due to the fact that the users often are supposed to incorporate in their system new programs which require knowledge of the problem, their use but also time and space for their integration in their computer. Moreover, after the integration, the users with dissatisfaction observe that they do not have access in a lot of pages in the internet, while, a lot of pages do not provide services in those that do not accept the application of cookies in their computers (Leenes & Koops 2005).

Finally, such mechanisms for data protection have been criticized as non adequate solutions to privacy threats. Some claim that “these technologies are insufficient: They solve only part of the problem and are open technical attacks, they are often difficult to integrate with the rest of the mass market content-distribution infrastructure, and they sometimes have unacceptably high costs” (Feigenbaum et al. 2001).

Although this claim was made at the beginning of the expanding use of technological protection measures for privacy, about a decade ago, they are still ongoing due to user’s ignorance or unwillingness to use PETs.

More particularly in the latest EU commission’s report on Pets it is found that “although survey evidence shows high levels of concern about privacy by individuals, there is little evidence that the demand by individuals for greater privacy is driving PETs deployment. In practice, individuals are faced with uncertainties about the risk of disclosure of personal data; a lack of knowledge about PETs; and behavioural biases that prevent individuals from acting in accordance with their stated preference for greater privacy” (Study on the economic benefits of privacy-enhancing technologies (PETs) (London Economics 2010)).

#### IV. New Initiatives

The above mentioned interconnection between DRMS and the private sphere have been widely recognised. As examples of such recognition and voices for change of the existing protection frameworks I will refer to two recent cases. The one is coming from a state initiative in Greece and the other is taken from the international level.

Firstly, the new project “Digital Greece 2020” is a permanent tool for consultation and formulation of policy proposals for the use of Information and Communication Technologies (ICTs) in critical sectors that will configure Digital Greece of 2020. The Forum aspires to formulate a policy proposal in line with the Digital Agenda 2020 of the European Commission that will utilize the current international experience, but will also thoroughly adapt it to the Greek reality. It has a dual presence, both physical and digital.

One of the working groups of this initiative is the “Interoperability, Free Software/Open Source Software (FS/OSS) and Open Content” group which has as an aim to contribute to the promotion of Free Software and Open Source Software, the adoption of the National Interoperability Framework as well as the diffusion of the benefits from the use of Open Standards. The work of the group is open to public consultation and participation on line via a specialized forum.

My main recommendations on the above mentioned problems have already been incorporated in the group's work and the latest ongoing group suggestions contain among others my recommendations for the amendment of the intellectual property law 2121/1993.

These recommendations focus mostly on the problem of privacy protection of those users that have the legal ownership of a copyright work and cannot exercise their right to fair use or any other exception of copyright due to the DRMS. Such mechanisms actually deprive the user from the right to make use of the exceptions of intellectual property the same way this could happen with a copyright work in the real world for example photocopying a book for private use. At the same time these mechanisms can violate his personal data.

According to these recommendations, the exceptions of copyright that exist in the real world should be also available for the internet. Therefore art 66 A5 on exception for private use should not include only “photocopy reproduction” but include any kind of technological reproduction.

Further, the circumvention of DRMS should be allowed in order to apply the exemptions of copyright in the internet. Their circumvention should be also accepted for reverse engineering of software from one form to the other the same way it is allowed in the Digital Millennium Copyright Act. This provision accepts the

circumvention from the legal owner of a program so as to achieve compatibility with other software in order for him to develop a legal copy.

Also, the circumvention of technological protection measures should be allowed when the measures used are violating personal data ex. for the creation of profiling. Such circumvention is allowed under the Digital Millennium Copyright Act.

In addition, a clear definition in the problematic notion of “effective measures” for copyright protection should be given since a number of problems in the implementation of the exceptions of copyright are being created. Finally, the implementation of intellectual property law in the internet should be followed in the framework of one intellectual property law so that it will not be a division between on line and off line protection.

Furthermore, the working group on open software has suggested a procedure of anonymising the data that are collected by the public administration compatible with the legislation on data protection law 2472/1997.

For this end, personal data are being divided in three categories. The first one contains information that could make a person directly identifiable. The most common example is a catalogue that contains lists of phone numbers, TIN etc. Such data should be prohibited in making public.

The second category includes the sensitive data which are clearly defined in the law 2472/97 art. 2b and include data on racial or ethnic origin, political views, religion or philosophical beliefs, participation in syndicates, health, social welfare, love life, data on criminal convictions or prosecution, participation in the relevant to the above unions of persons. Every data of this kind that can cause problems when linked to a certain person should be considered as sensitive.

Secondary data are those that do not belong in the previous categories, they do not reveal any especially sensitive information and do not imply the identity of the person with whom they are connected such as the age.

The data of the first category do not belong to the open data and should not be made public. The data of the next two categories cannot be published as such but can be turned into statistic data so as to be made public under the anonymisation procedure. In this anonymising procedure there should be a special provision so that the secondary characteristics of the persons such as age, address etc cannot lead to the identification of the persons.

Finally, another example on the concern of the civil society is the Resolution on Human Rights and Personal Data through which the Greek Section of Amnesty International is asking from the International Council of the Organization to prepare and present a comprehensive and inclusive policy for personal data as



defined by the relevant international conventions. The reasoning of the resolution is that “protection of privacy is crushed in the face of a hypothetical public interest in safety. This ignores the importance of privacy to the community and the effective exercise of other rights such as freedom of expression, freedom of assembly and association (...) Amnesty International should develop a detailed policy concerning use of personal data according to international human rights standards. We need to advocate the right to privacy on a political and operational level, demanding uncontrolled oversight so as to limit state agencies and private companies from storing and using personal data without consent” (Greece-Resolution 2010).

This evolution is very promising. Although privacy is a human right recognized by the international human rights instruments there is not an international movement for the protection of this right that has public recognition and numbers of activists. On the other hand the copyright industry employs a number of persons such as lawyers, counselors, journalists that stand up for the rights of the copyright holders and lobby for legislation that promotes their interest. It is worth mentioning that the Information Society Directive was also called as the “Most Lobbied Directive”. Indeed the number of interests involved on this directive that legalizes the use of technological protection measures was impressive. Representatives of the music industry, filmography, IT hardware and telecommunications as well as artists and writers’ groups were lobbying within the EU (Hart 2002).

## V. Conclusions

The statement of Jeffrey Cole in widespread press articles “There is no privacy in the internet. Get over it! We have to live our lives ready to see our dirty laundry on a cover” (Cole 2011) obviously creates great concern to internet uses. It is without doubt needed for the citizens to be aware of the possible violations of their personal data on the internet. When users are becoming aware of such dangers, the use of relevant technological methods so as to avoid such violations is increasing. It is also promising that new initiatives on data protection issues derive not only from the technological environment but also from the legal, academic environment and the civil society. It remains to be seen how effectively these dangers will be confronted.

Nevertheless, there is still conflict between the international nature of the technologies and the national nature of the relevant legislation for intellectual property and data protection. The initiatives of the EU, the US and WIPO do not always provide with sufficient answers to the problems. The harmonisation of these three levels is a prerequisite for the application of the exceptions of copy-

right without the obstacles of technological measures and without privacy violations.

Finally, in order to obtain further protection of privacy in the internet, the exchange of opinions in national and international level is needed as well as a constructive dialogue between the legislator, the industry and internet users. The wanted balance can be achieved through laws that are compatible with the new technological environment and the society's needs.

## References

The Economist, 31/5/1997

Jeffry Cole, interview to Nefeli Lygerou, K magazine 17/4/2011

Colin J. Bennet, Charles D. Raab, *The Governance of Privacy*, 2003

*Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys.*, 180 F.3d 1072, 1079 (9<sup>th</sup> Cir. 1999), footnote. 135(34)

Julie Cohen, DRM and Privacy, *Communications of the ACM*, Volume 46, Issue 4 (April 2003)

Serge Gutwirth, *Privacy and the Information Age*, Rowman and Littlefield Publishers, Inc (2002)

Peter Kleve & Richard De Mulder, Code is Murphy's Law, *International Review of Law Computers and Technology*, Vol. 19. No. 3 (2002)

Mathias Klang, Spyware: Paying for Software with our Privacy, *International Review of Law Computers and Technology*, volume 17, no. 3 (2003)

Diane Rowland & Elizabeth McDonald, *Information Technology Law*, Cavendish Publishing, 2005

Colin Bennett & Charles Raab, *The Governance of Privacy, Policy Instruments in Global Perspectives*, The MIT Press, 2003

Ronald Leenes & Bert-Jaap Koops, 'Code': Privacy's Death or Saviour?', *International Review of Law Computers and Technology*, Vol. 19, n. 3, pp. 329-340 (2005)

Andrea Ottolia, Preserving user's rights in DRM: dealing with 'juridical particularism' in the information society, *international Review of Intellectual Property and Competition Law* <http://www.digitalgreece2020.gr/en>

1.06 AI Greece ResolutionQ Human Rights and Personal Data, 16/4/2010 [www.petsymposium.org](http://www.petsymposium.org)

Joan Feigenbaum, Michael J. Freedman, Tomas Sander, Adam Shostack, Privacy Engineering for Digital Rights Management Systems, 2001

Daniel J. Solove, 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy, George Washington University Law School, San Diego Law Review, Vol. 44, 2007

Study on the economic benefits of privacy enhancing technologies (PETs) London Economics to The European Commission, DG Justice, Freedom and Security, 2010  
[Http://www.guardian.co.uk/technology/2009/jun/11/pirate-party-sweden](http://www.guardian.co.uk/technology/2009/jun/11/pirate-party-sweden)

M. Hart, The Copyright in the Information Society Directive: An Overview, European Intellectual Property Review, 2002, vol. 2, 58

# The scope of 'protective' European private international law rules in electronic consumer contracts: the Court of Justice of the European Union tackles the problem in the cases Pammer and Alpenhof

---

---

Bertel De Groote

---

---

## Introduction

ICT undoubtedly facilitates cross-border transfers of information. This contribution analyzes how their 'transboundary' characteristic influences the determination of the legal order applied to this information or to relations they led to.

The analysis takes into account some European private international law instruments. As far as international jurisdiction is meant, Regulation 44/2001 is taken into account. In order to determine the applicable law, one may refer to Regulation 593/2008 and Regulation 864/2007.

Starting point is the recent Judgment of the Court of Justice of the European Union in the so called *Alpenhof*-case<sup>1</sup>.

Through the analysis of and comments on the *Alpenhof*-case it has to be made clear what kind of information, available on an internet-platform, leads to the application of consumer protective PIL-rules in *Brussels I* and *Rome I*. The content as well as the presentation of the information will be taken into account.

Though the case concerns Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters<sup>2</sup> (hereinafter: *Brussels I* or *Regulation 44/2001*), of which art. 15 will be the focal point of this contribution, it seems evident that the judg-

---

1. Judgment in joined cases C-585/08 and C-144/09, 7 December 2010, *Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v. Oliver Heller*. The Judgment as well as the Opinion of Advocate-General Trstenjak, delivered on 18 May 2010, can easily be consulted on the website of the Court of Justice of the European Union (<http://curia.europa.eu>).

For the Judgment, see as well: *OJ C* 55, 19 February 2011, 4.

For a commented summary: R. Steennot, "Hof van Justitie preciseert bevoegd gerecht bij verkoop via internet", *Juristenkrant* 23 February 2011, 7.

2. *OJ L* 12, 16 January 2001, 1.

ment clarifies the application of *Regulation 593/2008* (hereinafter also called *Rome I*) as well<sup>3</sup>.

## Regulatory framework: Brussels I and Rome I

### *Brussels I*

Regulation 44/2001 comprises specific rules for consumer contracts. Being more favorable to the consumer 's interests than the general rules – laid down in art. 2<sup>4</sup> and 5 (1)(a)<sup>5</sup> - they have to protect him as the weaker party<sup>6</sup> in order to correct the presumed imbalance between consumer and trader.

Thus, consumer contracts are determined by a specific set of rules of jurisdiction.

They apply when the contract is concluded by a consumer, for a purpose which can be regarded as being outside his trade or profession, if it is a contract for the sale of goods on instalment credit terms or if it is a contract for a loan repayable by instalments, or for any other form of credit, made to finance the sale of goods.

Apart from these cases, in order for the protection to be accorded to the consumer, the contract has to be concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State<sup>7</sup>. Moreover the contract has to fall within the scope of such activities.

If the aforementioned conditions, laid down in art. 15, are fulfilled, according to art. 16 the consumer can bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or in the courts for the place where the consumer is domiciled.

Proceedings by the other party against a consumer however, may only be brought in the courts of the Member State in which the consumer is domiciled. Therefore

---

3. Comp. Recital 7 in the preamble to Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). See OJ L 177, 4 July 2008, 6.

4. Art. 2(1) *Brussels I* provides: "Subject to this Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State."

5. Art. 5(1)(a) *Brussels I* reads as follows: "A person domiciled in a Member State may, in another Member State be sued:  
(a) in matters relating to a contract, in the courts for the place of performance of the obligation in question."

6. Recital 13 in the preamble to *Regulation 44/2001*.

7. Or to several States including that Member State.

the consumer, whether defendant or actor, can never be deprived of the advantage of the “home player”<sup>8</sup>.

Interesting in this regard is the shift in the wording of the conditions for the applicability of the protective rules of private international law.

In the Convention of 27 September 1968 on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (hereinafter: *Brussels Convention*), art. 13(3) foresees the protection for contracts for the supply of goods or for the supply of services, whereby the conclusion of the contract was preceded in the State of the consumer’s domicile by a *specific invitation* to the latter or by *advertising*.

Moreover, the consumer must have taken the necessary steps for the conclusion of the contract in the concerned State.

### **Influence of the interpretation of Brussels I on the interpretation of Rome I**

As recital 24 in the preamble to *Regulation 593/2008* stresses the importance of *consistency* regarding the interpretation of the concept of ‘directed activity’ as a condition for the application of the consumer protection rule, it seems useful to expand the considerations regarding the interpretation of art. 15 *Regulation 44/2001* to *Regulation 593/2008*<sup>9</sup>. In both instruments the applicability of the

---

8. See: art. 16(2) *Brussels I*.

The jurisdiction rules do not affect the right to bring a counter-claim in the court in which, in accordance, with Section 4 (“Jurisdiction over consumer contracts”) of Chapter II (“Jurisdiction”) the original claim is pending.

Art. 17 *Brussels I* contains the conditions under which it can be departed from the provisions regarding jurisdiction over consumer contracts by an jurisdiction agreement.

Jurisdiction clauses have effect when parties entered into them after the dispute has arisen or when they allow the consumer to bring proceedings in courts other than those indicated in art. 16 – i.e. the *courts* of the Member State in which the consumer’s counter-party is domiciled or the *court* of the place where the consumer is domiciled (stressed by the author). Lastly the provisions of the Section regarding jurisdiction over consumer contracts may be departed from by an agreement which is entered into by the consumer and the other party to the contract when both are domiciled or habitually resident in the same Member State at the time of conclusion of the contract. Moreover the agreement must confer jurisdiction to the courts of the latter Member State and it may not be contrary to the law of the concerned State.

9. Art. 6 *Regulation 593/2008* guarantees consistency with *Regulation 44/2001* regarding the substantive scope of the consumer protective dispositions. The wording of art. 6 *Regulation 593/2008* is very close to art. 15(1)(c) *Regulation 44/2001*.

Nevertheless, while art. 15 *Brussels I* explicitly includes contracts on instalment credit terms (sale of goods on instalment credit terms or loan/other credit repayable by instalments, made to finance the sale of goods), regardless of where the activities in which framework they’re con-

consumer protective PIL-rules are depending on whether the trader, using an e-platform for his commercial activities, has directed his activities to the Member State where the consumer is domiciled/has his habitual residence.

Art. 6 Rome I, regarding *consumer contracts*, reads as follows:

“1. Without prejudice to Articles 5 and 7, a contract concluded by a natural person for a purpose which can be regarded as being outside his trade or profession (the consumer) with another person acting in the exercise of his trade or profession (the professional) shall be governed by the law of the country where the consumer has his habitual residence, provided that the professional:

- a) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or
- b) by any means, directs such activities to that country or to several countries including that country,

and the contract falls within the scope of such activities”.

Regarding this concept’s interpretation one may refer to a joint declaration by the Council and the Commission on Article 15 of Regulation (EC) No 44/2001.

It deals expressly with the applicability of private international law-rules, especially the aforementioned new European PIL-instruments, in an ICT-context.

According to this declaration the mere accessibility of an Internet site is not sufficient for Article 15 to be applicable. It would implicate that the trader has to be prepared to see himself confronted with the consumer protective rules on a global scale.

A factor will be however that this Internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance, by whatever means. Moreover, according to this declaration, the *language or currency which a website uses does not constitute a relevant factor* in this regard.

Thereto comes that the contract must be concluded within the framework of its activities.

Having this declaration in mind, the contribution will analyze the *Alpenhof*-decision. This will clarify where the interpretation given by the Court of Justice of the European Union confirms the Council and Commission’s view on the scope of art. 15, how this view has to be concretized and where nuances are necessary.

---

cluded are pursued or directed to, art. 6 *Rome I* apply to credit contracts – as mentioned in Brussels I – that do not fit within so-called directed/pursued activities.

### ***The Alpenhof-case***

#### **Criteria to assess whether a trader's activity is directed to a specific Member State**

The quintessence of the Court decision in the *Alpenhof*-case, concerns the determination of the criteria on the basis of which a trader can be considered to be *directing* his activity to the Member State of the consumer's domicile.

The Court especially addresses this question in an IT-context, more specifically to a case in which the trader's activity is presented on its website (or on its intermediary's website).

This may not however lead to the conclusion that art. 15(1)(c) is uniquely or even specifically applicable to e-contracts. Its wording doesn't preclude the application of the protective rules in view of the means by which a trader directs his activities to the consumer's Member State. Be it mass communication or individual communication, with use of a traditional or a 'new' communication platform,...the ratio for the protection doesn't seem affected. While its application seems most evident when distance contracts are at stake, one might even wonder whether art. 15(1)(c) cannot as well be invoked for contracts concluded in the presence of both parties if they fall within the scope of activities directed to the consumer's domicile. The latter activities, rather than the mode for the conclusion of the contract seem to determine the consumer's need to protection and influence the shift in balance between the consumer and the professional he contracted with.

In order to facilitate the understanding of the Court's reasoning, the elements that ought to be assessed can be shortly brought in mind.

In C-585/08, Pammer booked a voyage by post after he found out that it existed by consulting Reederei Karl Schlüter's intermediary's website and after having obtained further information from the latter by email.

In C-144/09, Heller contracted with Alpenhof after having found out that it existed by means of the internet, reserved and confirmed the reservation electronically as well.

In both cases it seems undoubted that the litigious contract falls within the scope of the trader's activities.



## Autonomous interpretation

As was the case with art. 13 *Brussels Convention*, art. 15 – replacing it – has to be interpreted, in view of its effectiveness, in an *autonomous* way, taking into account the objectives of the Regulation and in coherence with its system<sup>10</sup>.

While striving for continuity with the interpretation of the consumer protective rules of the Brussels Convention, the Court has to take into account the changes embedded in the wording of art. 15<sup>11</sup>.

Though the place nor the function – namely the protection of the consumer, considered being the weaker party – of art. 15 *Brussels I* differ from art. 13 *Brussels Convention*<sup>12</sup>, it has to be taken into account that the wording of art. 15 *Regulation 44/2001* differs from the wording of art. 13 *Brussels Convention*.

Though an adequate protection of the consumer is the common objective, art. 15 words the conditions for application of the protective rules in a more *general* way<sup>13</sup>.

This approach is particularly important in an electronic context, since its more open and general wording than the advertisement and specific invitation<sup>14</sup> required in art. 13 *Brussels Convention*, tends to ensure better protection for consumers with regard to new means of communication and the development of electronic commerce<sup>15</sup>. The interpretation given by the Alpenhof-decision, as analyzed underneath, has to illustrate so.

Do directed activities require the trader's intention?

---

10. Paragraph 55, referring to Court of Justice of the European Union C-96/00 (Rudolf Gabriel), 11 July 2002, *ECR* 2002 I-6367, par. 37.

11. Paragraph 56.

12. Recital 13 of the preamble states that in relation to insurance, consumer contracts and employment, the weaker party should be protected by rules of jurisdiction more favourable to his interests than the general rules provide for. See in this regard as well: Court of Justice of the European Union C-180/06 (*Renate Ilsinger v. Martin Dreschers*, acting as administrator in the insolvency of Schlank & Schick GmbH), 14 May 2009, *ECR* 2009 I-3961, par. 41.

13. In this regard paragraph 58 refers to Court of Justice of the European Union C-27/02 (*Petra Engler v. Janus Versand GmbH*), 20 January 2005, *ECR* 2005 I-481, par. 39 and Court of Justice of the European Union C-464/01 (*Johann Gruber v. Bay Wa AG*), 20 January 2005, *ECR* I-458, par. 34.

14. One could contend that only an email addressed to the consumer could be doubtlessly seen as a specific invitation.

15. Compare: Court of Justice of the European Union C-180/06 (*Renate Ilsinger v. Martin Dreschers*, acting as administrator in the insolvency of Schlank & Schick GmbH), 14 May 2009, *ECR* 2009 I-3961, par. 50.

Regarding the trader's behavior, the necessity of a specific invitation addressed to the consumer or advertisement in the State of the latter's domicile is now replaced by the requirement that the trader – whereby the conditions of applicability concern him alone – pursues its commercial activities in the Member State of the consumer's domicile or directs such activities to that Member State or to several States, including that Member State<sup>16</sup>.

Of specific relevance for the electronic environment seems the addition 'by any means', since the medium/platform or the communication tools that are used may not affect the conclusion whether activities are 'directed' to a specific State or not.

More important however seems the technology-neutral notion 'directed activities' in itself. If read jointly, its open wording is stressed by the words 'by any means'. As the Court states, while art. 15 encompasses and replaces the concepts used in the *Brussels Convention*<sup>17</sup> it thus covers a wider range of activities<sup>18</sup>. Since not requiring a predefined content or format of behavior and information on the trader's side, it admits advertisements or specific invitations as meant in art. 13 *Brussels Convention* as elements that establish directed activities without limiting the list of elements that can prove such activity to them.

The idea that the development of internet communication increases the vulnerability of consumers with regard to traders' offers seems to be at the origin of this broader approach. Nonetheless, this need doesn't affect the need for protection for consumer confronted with more traditional, or must one say old-fashioned, means to direct activities to their home States. As soon as activities are directed to a certain market, by whatever means, the power-balance seems that much broken that protective rules have to re-install the equilibrium. Therefore, while the concepts 'advertisement' and 'specific invitation' seem especially in an e-context too narrow, in a more traditional context the power-balance can be ruptured by initiatives from/on behalf of the trader that do not specifically fit within the concepts used in art. 13 *Brussels Convention*.

Though the scope of art. 15 *Brussels I* may be broader than the reach of art. 13 *Brussels Convention*, it remains unclear however whether this increase requires an interpretation whereby the words 'directs such activities' encompasses an activity that is *de facto* turned towards one or more Member States or that the intention of the trader to do so has to be involved as well<sup>19</sup>.

---

16. Moreover, the contract must be within the scope of the concerned activities.

17. In this regard, see art. 13.

18. Paragraph 61.

19. Paragraph 63.

In the latter scenario it will have to be determined in what form this intention must manifest itself in an electronic context.

A major difference between advertising by means of the internet and in a classic form<sup>20</sup> concerns the outlay of expenditure – that can be significant in the latter case – by the trader in order to make itself known in other Member States. This expenditure demonstrates the trader's intention.

The worldwide reach of communication is on the contrary inherent to the internet. Therefore the aforementioned intention cannot be derived from the worldwide accessibility of webvertisement.

The Court of Justice expresses this idea as follows:

“Since this method of communication inherently has a worldwide reach, advertising on a website by a trader is in principle accessible in all States, and, therefore, throughout the European Union, without any need to incur additional expenditure and irrespective of the intention or otherwise of the trader to target consumers outside the territory of the State in which it is established”<sup>21</sup>.

Though advertisement by means of the internet – contrary to other forms of advertisement - doesn't automatically implicate the 'intention' to be present on the markets of all the States where the advertisement can be seen, the mere accessibility of a website has not to be seen as in line with the words “directs activities to”. This doesn't have to be contrary to the statement that the latter concept may be broader than the notion 'advertisement'. The accessibility of webvertisement in a Member State, while there are no indications that the advertiser wanted to affect to market in the concerned State, does not meet the condition, set out in art. 13(3)(a) *Brussels Convention* that the conclusions of the contract has to be preceded in the State of the consumer's domicile by advertising. The same can be defended *a fortiori* if there are indications that the advertisement didn't intended to reach that State. This is the case for instance if the trader expressly limits the geographical scope in the advertisement itself.

---

20. See: Court of Justice of the European Union C-96/00 (Rudolf Gabriel), 11 July 2002, *ECR* 2002 I-6367, par. 44. According to this Court decision art. 13 *Brussels Convention* covers all forms of advertising carried out in the Contracting State in which the consumer is domiciled, whether disseminated generally by the press, radio, television, cinema or any other medium, or addressed directly, for example by means of catalogues sent specifically to that State, as well as commercial offers made to the consumer in person, in particular by an agent or door-to-door salesman.

21. Paragraph 68.

Another assessment of 'accessibility' of information leads to the risk that the consumer protection gets an absolute character<sup>22</sup>. So, it wouldn't have sense to limit the application of the protective rules to the direction of the trader's activities to a Member State.

In this regards, one can mention the Advocate General's observation that in view of a teleological interpretation of the litigious concept, the interests of the consumer and of the trader, who wants to avoid jurisdiction in the place of the consumer's domicile if he hasn't knowingly directed his activities to that Member State, have to be balanced. Protection of the consumer therefore requires sufficient connectivity between the contract and the Member State of the consumer's domicile<sup>23</sup>. If the European legislator on the contrary shared the opinion that the ICT-environment *in se* made the consumer's protection indispensable he'd have drafted art. 15 differently, rather referring to accessibility. Since this is not the case, one may conclude that mere presence on the internet – accessibility of a website – does not trigger the consumer protection rules.

The Court clarifies that whilst seeking to confer further protection on consumers, the European Union legislature did not go as far as to lay down that mere use of a website, which has become a customary means of engaging in trade, whatever the territory targeted, amounts to an activity 'directed to' other Member States<sup>24</sup>.

---

22. See in this regard paragraph 70, referring to Court of Justice of the European Union C-215/08 (*E. Friz GmbH v. Carsten von der Heyden*), 15 April 2010, par. 44 [to be consulted electronically on the website of the Court of Justice of the European Union (<http://curia.europa.eu/>) or via Eur-Lex (Access Portal to European Union Law - <http://eur-lex.europa.eu/>)], concerning Council Directive 85/577/EEC of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises (see: *OJ L* 37, 31 December 1985, 31).

23. Advocate General Trstenjak in paragraph 64 of his opinion subscribes in this regard – correctly – the point of view of the Netherlands government.

24. Paragraph 72. One may mention in this regard paragraph 73 of the Court decision and footnote 37 of Advocate-General TRSTENJAK's Opinion of 18 May 2010.

It has to be mentioned that the European Parliament amended the Commission's proposal in a sense that comforts the Advocate General's opinion. The Parliament suggested the wording that electronic commerce by a means accessible in another Member State constitutes an activity directed to that State where the on-line trading site is an active site in the sense that the trader purposefully directs his activity in a substantial way to that other State (*OJ C* 146, 17 May 2001, 97)(See: European Parliament legislative resolution on the proposal for a Council regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (COM(1999) 348 - C5-0169/1999 - 1999/0154(CNS)), *OJ C* 146, 17 May 2001, 101).

Accessibility can therefore not be seen as a manifestation of the intention to establish commercial relations with 'foreign' consumers, necessary for the involvement of consumer-friendly rules<sup>25</sup>.

In this regard reference can be made to a joint declaration by the Council and the Commission on Article 15 of Brussels I<sup>26</sup>, echoed in recital 24 of the preamble to *Rome I* since it states that for article 15(1)(c) to be applicable it is not sufficient for an undertaking to *target*<sup>27</sup> its activities at the Member State of the consumer's residence, or at a number of Member States including that Member State; a contract must also be concluded within the framework of its activities.

Moreover, and more relevant for the sake of this analysis, the Council and the Commission clarify that the mere fact that an internet site is accessible is not sufficient for article 15 to be applicable, although a factor will be that this internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance, by whatever means. The wording of the joint statement clarifies as well that the mere conclusion of a contract doesn't necessarily mean that the contract was solicited for. Both elements, the contract and the directed activity it fits in, have to be present in order to meet the conditions of applicability set out in art. 15.

The joint statement confirms the interpretation that the use of ICT has to give evidence of the intention to establish commercial relations in the Member State of the consumer's domicile. The conclusion of a contract with a consumer therefore has to be preceded by elements that demonstrate that the trader 'envisaged' doing business in the concerned state, i.e. minded to conclude contracts with consumers there<sup>28</sup>.

The Court of Justice of the European Union is brought to a two-step reasoning. After having determined that activities can only *intentionally* be directed, the Court draws up an exemplary list of elements that indicate this intention. It gives way to criteria to assess the trader's information about his activities as well as how that information is transferred and presented.

---

25. Paragraph 75.

26. Statement of the Council and the Commission on Articles 15 and 73 of Regulation 44/2001. The statement can be consulted on the website of the European Judicial Network in civil and commercial matters (<http://ec.europa.eu/civiljustice>). Follow the hyperlink: [http://ec.europa.eu/civiljustice/homepage/homepage\\_ec\\_en\\_declaration.pdf](http://ec.europa.eu/civiljustice/homepage/homepage_ec_en_declaration.pdf). Last consultation of the site: 30 May 2011.

27. Stressed by the author.

28. See in this regard paragraph 76.

### ***Elements establishing a directed activity: the Alpenhof-assessment***

#### **Black list**

In order to assess the use of ICT, especially the information it bears and how this information is presented, the *Alpenhof*-decision inspires to a three-layered approach. In order to clarify the assessment this contribution introduces a black, white and grey list of elements.

In paragraph 77 of the *Alpenhof*-decision the Court of Justice of the European Union clearly excludes some mentions on a trader's website from being evidence that the trader envisaged doing business abroad.

The exclusion concerns :

– the trader's email address

or

the trader's geographical address

or

– the trader's telephone number without an international code.

This exclusion can be justified as this information is as necessary for a consumer domiciled in the Member State where the trader is established –especially in view of a distance contract - as a consumer from abroad needs it to get in touch with the trader. This type of information therefore can be considered as neutral for the assessment of the trader's intention.

Thereto comes that the Directive on electronic commerce contains a general information duty and requires the provider of information society services to disclose at least the geographic address at which the service provider is established and details – including the service provider's electronic mail address – allowing him to be contacted rapidly and communicated with in a direct and effective manner<sup>29</sup>.

This duty to disclose contact information is independent of the Member State the trader directs its activity to. It therefore also concerns a trader whose activity is to be qualified as purely 'national'.

---

29. See art. 5(1) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ L 178, 17 July 2000, 1*. Compare in this regard: Court of Justice of the European Union C-298/07 (*Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. deutsche internet versicherung AG*), 16 October 2008, *ECR 2008 I-7841*, par. 40.

Neither decisive seems the 'interactive' character of an ICT-platform, enabling contracts to be concluded electronically, or even the question whether or not a trader can be contacted electronically (through the platform)<sup>30</sup>.

The 'interactivity' of a website is not an effective measure of the intended character of the extraterritorial nature of the activities it sustains.

On the contrary, the fact that contact details – be it a geographical address or an electronic address – are mentioned, allows the consumer to inquire with the trader in view of entering in a contractual relation. This opportunity does not however in se proofs the trader's intention to give its activities an extraterritorial grab. In the same line of reasoning the so-called passive character of a website does not preclude this site from containing information that gives evidence of the trader's intention to develop activities in (a) certain State(s).

In this regard the Court of Justice of the European Union's *Alpenhof*-decision refines the explanatory memorandum in the Proposal of the Commission of the European Communities for a Council regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters regarding art. 15<sup>31</sup>.

The latter seems to connect the applicability of the consumer protective jurisdiction rule (art. 15 (3)) with consumer contracts that are concluded via an interactive website that is accessible in the Member State of the consumer's domicile. A passive website, accessible in the State of the consumer's domicile, giving this consumer knowledge of a service or of the possibility to buy goods, does, according to the memorandum, not trigger the protective jurisdiction.

Since the memorandum focuses on a passive site that simply contains information that allows the consumer to enter into a contract<sup>32</sup>, that information's character rather than the passive character of the website seems to drive it to the conclusion that 'directed activities' are lacking.

---

30. Compare: J.-P. Moyné, B. De Groote, "Cyberconsommation' et droit international privé", *R.D.T.I.* 2009, 30.

31. Proposal for a Council Regulation (EC) on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (COM(1999) 348 final — 1999/0154(CNS)), submitted by the Commission on 7 September 1999, OJ C 376 E, 28 December 1999, 1. For the explanatory memorandum (see specifically p. 16), the text can best be consulted on the website of Eur-Lex via the hyperlink: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1999:0348:FIN:EN:PDF> (last consulted 15 June 2011).

32. The so-called passive site in its purest form contains information, accessible for the visitor. In this site no tools that allow the visitor to communicate with its owner or to place an order are embedded. The contrary goes for interactive sites. Seen on a scale the degree of interactivity can vary depending on the site's functionalities.

The memorandum links its assessment of an interactive site to the concept 'directed activities'. This stresses the technology-neutrality of the condition for the application of the specific jurisdiction rules for consumer contracts. It enables the memorandum to state that the ICT-driven medium, though it clearly facilitates extra-territorial commercial relations and the conclusion of cross-border contracts, doesn't lead to another treatment than the treatment of contracts concluded by phone or fax. The latter as well have to be concluded within a framework of activities directed to the consumer's Member State. Moreover, as far as the interactive site illustrates the trader's intention to solicit business in a State a contract that is not concluded by means of that site (for instance by another communication tool for distance contracts), but nevertheless in the framework of the mentioned activities, the application of art. 15 *Regulation 44/2001* is triggered as well.

### White list

On the other hand the Court of Justice of the European Union seems to draw up a non-exhaustive white list. It contains what the Court considers being 'clear' expressions of the intention to solicit the custom of consumers in a specific State<sup>33</sup>.

Evidence of a 'directed' activity includes for instance<sup>34</sup>:

- the mention that the trader is offering services or goods in (a) Member State(s) designated by name;
- The disbursement of expenditure on an internet referencing service to the operator of search engine, in order to facilitate access to the trader's site by consumers domiciled in various Member States<sup>35</sup>. The validity of the Court's reasoning in this regard is limited however to services that themselves have a scope that covers the Member State in which the concerned consumer is domiciled. This means that their activity has to be directed to that Member State in order to be able to contribute to the reach of the referenced website in this State.

### Grey list

While evidence as mentioned in the white list is patent, a third, grey list may contain other items of evidence that are – alone or combined – demonstrating 'directed' activity.

---

33. See paragraph 80.

34. The examples are taken from paragraph 81.

35. Paragraph 81.



Hereby the idea that the direction that is given to an activity can only be established by patent evidence is overthrown by the Court of Justice of the European Union<sup>36</sup>.

Inspired by the factual context of the main proceedings that led to the preliminary proceedings, the Court enumerates in a non-exhaustive way, some elements that “are capable of demonstrating the existence of an activity ‘directed to’ the Member State of the consumer’s domicile”<sup>37</sup>. One may note – as explained before – that the relevancy of this ‘information’ is not limited to art. 15(1)(c) Brussels I, but also concerns the Rome I that is in this regard worded identically. Moreover it is justified to assess this ‘information’ in an identical way.

### International character of the activities

In paragraph 83 the Court of Justice of the European Union first of all mentions the international character of the activity at stake.

One may defend that tourist activities as developed by Reederei Schlüter and hotel Alpenhof may be considered as having a transnational character. It is interesting to note in this regard that the Court, given the facts of the main proceedings, expressly mentions *certain* tourist activities as having an international nature.

Activities in tourism – even if related to different countries (i.e. voyages by freighter from Europe to Asia as in the *Pammer*-case) – do not *per se* aim at foreign markets<sup>38</sup>. This doesn’t exclude them from being relevant evidence on the contrary. To assess the activities’ scope other evidence regarding the scope of the activities has to be taken into account as well.

Nevertheless, tourist activities – even if the services are rendered abroad, which is quite common in this sector – can as well be pursued only in one country, i.e. where the trader is established. The location of the service delivery, i.e. where the journey leads to, is not to be confounded with the market the trader directs activities to. The market share strived for can be purely ‘internal’. While the offer is national, the services the tourist activities consist of can be rendered globally.

---

36. See paragraph 82, where the Court considers that the European Parliament by its legislative resolution on the proposal for *Brussels I* rejected wording stating that the trader had to purposefully direct his activity in a substantial way to the Member State of the consumer’s domicile.

37. Paragraph 83.

38. Comp. Paragraph 90.

## Telephone numbers with international codes

An indication for the Court is as well the fact that telephone numbers with an international code are mentioned<sup>39</sup>. The international code can be seen as information that is expressly meant to give international customers easy access to the trade. Therefore, the reasoning of the Court seems to be, that this information has to be assessed as a way to 'invite' foreign customers<sup>40</sup>, thus expanding the reach of the trader's activities to (a) foreign market(s).

## Domain names

Top-level domain names can be seen as an indicator for the trader's extraterritorial ambition/intention as well, namely if they differ from the one of the Member State in which the trader is established<sup>41</sup>.

One may wonder whether the Court doesn't overestimate the relevance of top-level domain names as an indication of the international ambit of a trader, especially when neutral top-level domain names are involved.

Other characteristics of the trader's behavior have to be taken into account to assess whether the latter are part of the expression of the trader's intention to reach foreign markets and if so to determine whether the scope of its activities can be connected to specific countries. The same goes for the use of some 'exotic' top-levels. Though linked to a country they can be seen as the flag-state of activities with an international or even global reach. Complexity will even be added to the debate when top-level will be linked to regions rather than countries.

One may therefore wonder whether domain names must not mainly combined with other elements rather than being *in se* a good indicator for a commercial activity that is directed to another State than the one in which the trader is established.

## Description of itineraries

Fourthly, the Court of Justice of the European Union considers the description of itineraries from (an) other Member State(s) to the place where the service is provided as evidential<sup>42</sup>. A 'How to reach us' or 'How to get there', informing customers coming from abroad about the right itinerary to where the service is

---

39. Paragraph 83.

40. Though not necessary being a specific invitation as meant in art. 13 *Brussels Convention*.

41. Paragraph 83.

42. Paragraph 83.

delivered proofs the trader's intention to direct his activities to the State in which the itinerary's 'point of departure' is located.

## Language and currency

In a joint statement on articles 15 and 73 Brussels I, the Council and the Commission expressed serious doubts regarding the relevancy of the language used on an ICT-platform<sup>43</sup>. Neither the used currency was seen as decisive information to evaluate a website as soliciting the conclusion of distance contracts (with consumers in Member State than the one in which the trader is established).

This approach was echoed regarding the applicable law on contractual relations – and especially the applicability of the consumer-friendly choice-of-law rules in art. 6 – in recital 24 of the preamble of *Rome I*.

The Court of Justice of the European Union in consideration 84 subscribes this point of view, as far as languages are concerned that are generally used in the Member State from which the trader pursues its activity.

The fact that a website contains information in German is not to be seen as an element to establish the trader's intention to direct activities to another country where German is generally used, Austria for instance, if the trader pursues its activity from Germany, or more generally spoken from a country where this language – German – is generally used. In the Alpenhof-case, the website in German does not establish the intention of the Austrian hotel to attend clients in another German-speaking country, *in casu* Germany.

One may defend an analogous reasoning for the relevancy of the currency that is mentioned on a website.

Moreover, within the European Union account has to be taken of the Eurozone. In order to determine the intention of a trader, established in the Eurozone, to reach with his business other Eurozone countries the used currency – i.e. the Euro – seems not decisive. On the other hand the use of the Euro on the website of a trader pursuing activities from a State where another currency is used can be seen as an indicator of his intention to be active on the market of the Eurozone States

---

43. Statement of the Council and the Commission on Articles 15 and 73 of Regulation 44/2001. The statement can be consulted on the website of the European Judicial Network in civil and commercial matters (<http://ec.europa.eu/civiljustice>). Follow the hyperlink: [http://ec.europa.eu/civiljustice/homepage/homepage\\_ec\\_en\\_declaration.pdf](http://ec.europa.eu/civiljustice/homepage/homepage_ec_en_declaration.pdf). Last consultation of the site: 30 May 2011.

or one/some of them<sup>44</sup>. To determine whether all or only some Eurozone States are 'targeted' a combination of elements seems necessary. Information thus will have to be assembled.

Lastly one may wonder whether the use of English in a website, though by a trader pursuing activities from a country where it is not an official language/not generally used, can be seen as a decisive indicator – at least when not combined with other information – to target other countries.

English is a very prominent language on the internet and therefore it could, without complementary information, be seen as a non-distinctive characteristic.

In this line of reasoning the use of English should not in itself be seen as establishing the trader's intention to target countries where English is generally speaking. If it should, other elements would be necessary to determine which particular English-speaking countries fall within the trader's scope. On the other hand, the use of this language should not oppose the conclusion that the trader – if other elements in this sense are present – is directing his activities to a State where English is not generally speaking.

The presumption that all internet users can feel addressed if information is in English, because of the prevalence of this language on the internet, justifies the requirement of complementary elements.

A cautious approach of the use of this language is a prerequisite to avoid that the application of the consumer protective private international law rules can be claimed almost globally.

From this point of view, the use of the English language can better be seen as a weak indicator for the intention to reach countries where English is generally spoken. Otherwise the major role of this language in activities on the net than to easily qualify its use as an indicator for the intention to reach all countries.

Notwithstanding this remark, the Court - though (f.i. in the *Pammer*-case) in a context where the language of the website was the trader's language as well – considered that if the website permits consumers to use a *different* language or a *different* currency, the language and /or currency can be taken into consideration.

---

44. The assessment requires great care, since the situation might even be more complex. If a trader, pursuing activities from a Member State (whether part of the Eurozone or not) uses the USD as currency this is, due to the global role of this currency, not in itself a reason to exclude EU-countries from the reach of those activities. The use of the Euro can, for the same reason – especially since lot of websites integrate payment by credit card in their website – not in itself be seen as an exclusion of Member States out of the Eurozone or even third countries from the activities' scope.

This means that it can constitute evidence from which it may be concluded that the trader's activity is directed to other Member States<sup>45</sup>.

Anyhow, the wording used by the Court of Justice of the European Union seems not contrary to the care we suggested when assessing the aforementioned elements.

According to the court they *can* be taken into consideration and they *can* constitute evidence from which the trader's intention may be concluded.

Moreover, the Court clearly mentions that the website – of the trader or its intermediary – *and* the trader's overall activity must make apparent that the trader envisaged doing business in the Member State of the consumer's domicile<sup>46</sup>.

Such a *combined* assessment seems very useful as factors as the use of English as the website's language or the use of a widespread currency may on the one hand contribute to the international character of the site, but seems on the other hand non-decisive or neutral regarding the specific countries the activities aim at.

### **International clientele and its comments**

Lastly, the Court of Justice of the European Union mentions in paragraph 83 the trader's mention of an international clientele, composed of customers domiciled in various/a Member State(s) different from the one where the trader is established, as an item of evidence capable of demonstrating an activity that's directed to the concerned Member State(s).

For the Court this information is particularly relevant if the international nature of the trader's customers can be demonstrated by accounts written by them.

If the international clientele is presented by means of information originating from them and concerning their evaluation of the trader's products/services, the pretention that activities are directed to them gains is strengthened as it is based on information regarding their contract(s) with the trader.

It's neither excluded that the mentioned clientele can, depending on the wording, be an element that sustains the conclusion that activities are directed to all or different Member States. Therefore other elements concerning the business' scope can be relevant. This is even possible in cases where the international clientele referred to doesn't include customers in the targeted Member States<sup>47</sup>. In this

---

45. Paragraph 84.

46. See paragraph 92.

47. The concrete wording can thus be an element that sustains the conclusion that the activities of the trader are directed beyond the concerned Member States (i.e. the Member States in which the mentioned clientele is domiciled).

case, other elements may be required however to establish the existence of activities directed to the concerned countries. It has to be remarked as well that this information is an element that sustains the conclusion that the concerned activity has an international character.

On the other hand, mentioning a broad clientele can as well lead to the conclusion that the international activities simply lack a direction<sup>48</sup>. In that case, the international elements seem non-decisive or neutral. As defended above, the qualification of the activities as directed to (a) specific Member State(s) or not will depend on other elements. They'll be relevant to determine the business' scope.

## Conclusion

The main importance of the *Alpenhof*-decision concerns the balance the Court of Justice of the European Union sought between the consumer's justified need for protection on the one hand, and the trader's quest for a legal framework that enables him to foresee the effects of the activities he develops by means of ICT.

Therefore the Court considered that the accessibility of a website is not a sufficient element to establish the 'directed' character of activities.

Since websites are globally accessible<sup>49</sup>, this interpretation would seriously undermine the relevance of the criteria of applicability set out in art. 15(1)(c) *Brussels I* and art. 6 *Rome I*.

The consumer may therefore only invoke protection if the trader *intentionally* develops business activities in the Member State of the consumer's domicile/place of residual residence. The contract must therefore be framed in an initiative of the trader to be active on the concerned market. This implies as well that the trader may not be taken by surprise.

As mere 'web-presence' – accessibility – does not meet the burden set out by *Brussels I/Rome I*, the Court embraced the idea that on a case-driven basis the presence of elements establishing 'directed activities' has to be assessed. The elements listed in the *Alpenhof*-case have to be considered as a non-exhaustive list of relevant indicators, based on the trader's presence on the internet.

---

48. This conclusion may even not be excluded if there is a reference to clientele of (a) specific Member State(s). The wording can be that 'flat' that the references nevertheless illustrate a broad approach. That approach must not necessarily be *directed*.

49. In principle, websites have a global character. Nevertheless the trader can take measures to limit the territorial scope of the website and consequently of his activities.

Since the mere accessibility of a website is not sufficient to trigger the specific protective PIL-rules for consumers, a passive website can in itself not lead to the conclusion that the trader is directing his activities to where it can be consulted.

This doesn't mean however that an interactive website is in itself a synonym for 'directed activity'. The Court of Justice of the European Union's decision is especially important where it denies the relevancy of the passive/interactive character of a website.

Taking the above mentioned considerations into account, it is undeniable that the conditions of applicability of the consumer protective PIL-rules have some shadow sides.

Striving for an equitable balance between the interests of consumer and trader, the interpretation given in the *Alpenhof*-case could lead to frustration. While considered too broad by the trader, the conditions of applicability might be seen as too friendly for the professional by the consumers.

The lack of an interpretation that clearly favours the consumer or the trader might not surprise however. The Court however wants to avoid an interpretation of the notion 'directing activities' that discourages traders from using ICT-platforms for developing their business (abroad). A too narrow interpretation on the contrary might negatively affect the consumer's willingness to enter in transactions on the internet.

The importance of the scope of the protective PIL-rules for the development of the e-commerce may therefore not be underestimated. It has to be noted that, in the autumn of 2010, the European Commission launched a consultation regarding the need to revise the directive on e-commerce of June 13 2000<sup>50</sup>. It hereby acknowledged that ten years after the adoption of the directive, the development of retail electronic commerce remains limited to less than 2% of European total retail trade. The critical analysis this contribution gave of the protective PIL-rules, and especially their conditions of applicability, in the "European" PIL-instruments therefore has to be considered against this background as well.

---

50. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, July 17 2000, 1-16). Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on Electronic commerce (2000/31/EC)). The consultation can be found on the European Commission's EU Single Market thematic website. An electronic version is available on [http://ec.europa.eu/internal\\_market/consultations/docs/2010/e-commerce/questionnaire\\_%20e-commerce\\_en.pdf](http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/questionnaire_%20e-commerce_en.pdf) (last consultation June 1, 2011).

# Mass digitisation and the moral right of integrity

---

Maurizio Borghi

---

Author's moral rights seem to have hard-living in the digital age. In spite of the often repeated statement that moral rights should become one of the central issues in the international debate on digital copyright, the legislative initiative in the field has been so far lazy, to say the least. To be sure, international bodies and governments have been very reactive to adapt economic rights to the challenges of new information technologies. By contrast, no significant initiative has been taken regarding moral rights. Both the TRIPs Agreement of 1994 and the WIPO Copyright Treaty of 1992 are silent on moral rights. At European level, moral rights have not been addressed in the seven directives constituting the *aquis communautaire* and are expressly excluded from the scope of the Information Society Directive 2001/29/EC<sup>1</sup>. Thus, with the sole exception of the WIPO Performances and Phonograms Treaty of 1996, which mandates for the extension of the moral rights of attribution and integrity to performers<sup>2</sup>, the international legislator has been completely silent on moral rights from far before the beginnings of the digital age. To date, the Berne Convention of 1886 – lastly amended exactly 40 years ago<sup>3</sup> – is still the most important and almost unique international legal instrument in the field. Art. 6 bis, which was first introduced in the Convention at the Rome Conference of 1928 after prolonged controversies<sup>4</sup>, recognises two relevant moral rights, namely paternity (or attribution) and integrity. However, no special provision has ever since been enacted to address the respect of moral rights in the digital environment.

One of the reasons of this void is certainly the lack of a general feeling of urgency in this matter. Digital technologies and the networked environment have

---

1. See Rec. 19.

2. WPPT, art. 5.

3. Berne Convention for the Protection of Literary and Artistic Works of 9 September 1886; lastly revised in Paris, 24 July 1971.

4. See Sam Ricketson & Jane Ginsburg, *International copyright and neighbouring rights: the Berne Convention and beyond*, 2nd ed., OUP 2005, pp. 223-230.



dramatically facilitated the way by which copyright works are *reproduced* and *distributed*. This has obviously had an impact on the two major economic rights of copyright, namely reproduction and distribution, and the legislator's promptness to expand the scope of these rights came with no surprise. As far as the European harmonisation process is concerned, moral rights were mentioned in the Green Paper of 1995 as one of the issues that, with the advent of the information society, were deemed to become more urgent than before<sup>5</sup>. In a Follow up of 1996, the Commission informed that an overwhelming number of interested parties had stressed the importance of moral rights in the digital environment, and particularly the right of integrity, and recommended further studies on the issue<sup>6</sup>. Yet, in 2000, a comprehensive study carried out by Salokannel and Strowel on behalf of the Commission concluded that, although the level of protection of moral rights differs significantly amongst Member States, there is no evidence that the existing differences affect the functioning of internal market. The study discouraged legislative initiative in the field and recommended the adoption of "soft law" mechanisms, such as good practices, as a more appropriate instrument to address the respect of moral rights in the digital environment<sup>7</sup>. As a result, the Information Society Directive passed on 2001 by leaving moral rights outside of its scope.

Certainly, this lack of initiative in the part of the world where moral rights are supposed to be championed has deeply affected the international legislation process. However, the overall negligence on this matter has still another explanation. Digital network technologies have caused new forms of creating and using works to become prominent. In this respect, the "cyber-space" has been described as dominated by large scale peer-production instead of centralised information production<sup>8</sup>, re-mix or "read-and-write" (RW) culture instead of "read only" (RO) culture<sup>9</sup>, briefly a space where the notional concepts of the public sphere are fat-

---

5. Green Paper on Copyright and Related Rights in the Information Society, European Commission Report, COM (95) 382 final, 19 July 1995, p. 29.

6. Follow up to Green Paper on copyright and related rights in the information society, European Commission Report no. COM (96) 568 final, 20 November 2006.

7. Marjut Salokannel & Alain Strowel (with the collaboration of Estelle Derclaye), Study contract concerning moral rights in the context of the exploitation of works through digital technology, Study contract n° ETD/99/B5-3000/E°28, Final Report, April 2000.

8. See Yochai Benkler, "Sharing Nicely: On Shareable Goods and the Emergence of Sharing as a Modality of Economic Production", 114 *Yale L.J.* 273 (2004); Erez Reuveni, "Authorship in the Age of the Conductor", *Journal of the Copyright Society of the U.S.A.* 1801(2007).

9. Lawrence Lessig, *Remix. Making Art and Commerce Thrive in the Hybrid Economy*, Penguin Press 2008. For the opposite view of Lessig's, see generally Spinello & Bottis, *A defense of intellectual property rights* 2009.

ed to blur. Along this line, commentators have extensively emphasised that the cyber-space challenges the traditional concepts of authorship, work and use, upon which copyright norms are framed. For instance, it is commonly observed that the world wide web tends to promote forms of collective authorship (e.g. Wikipedia) that do not fit well the copyright notion of “the author”. Similarly, works are less used in a purely consumptive way, and are increasingly transformed and re-used in a more or less creative way, so that a more “cavalier” approach towards work’s integrity and attribution is already adopted in practice. In order to take full advantage of peer-production and re-mix culture, certain barriers of copyright should be removed. Based on this background, “traditional” author’s moral rights seem to have become, as Guy Pessac has put it, “*persona non grata* within the cyberian discourse”<sup>10</sup>. As a matter of fact, scholars who have addressed the issue of moral rights in the digital environment have mainly advocated for a narrower construction of their scope<sup>11</sup>.

### Mass digitisation projects as a new challenge to moral rights

Yet with the advent of mass digitisation projects the scenario has changed. Mass digitisation is the conversion of works in digital format on an industrial scale. Projects such as Google Books, Internet Archive or Europeana, just to mention the most popular ones, come with the unprecedented and well-trumpeted promise to resuscitate the dream of the great library of Alexandria. As a matter of fact, mass digitisation projects are engaged in the mission of transplanting the whole cultural heritage of humankind, as deposited in books and in other physical carriers, in the digital network environment. Millions of items that carry works born in the pre-digital era are turned into sequences of bites that form part of the cyber-space. In this way, mass digitisation of cultural heritage does not only improve the quantity of information that is available in the cyber space, but it adds to the cyber space something that the latter would have never produced on its own. The to-be-digitised works are not “products” of the cultures of the cyber-space; they are, rather, transplanted into the cyber-space by virtue of a mechanical operation. Works are transplanted from a context to another. We may define as “authorial context” the environment from where they originate, and “cyber-context” the environment to which they are transplanted by effect of mass digitisation.

In the authorial context, works are, so to speak, *dense* units. Books are not just accidentally physical containers of information that would otherwise flow un-

---

10. Guy Pessach, “The author’s moral right of integrity in cyberspace - a preliminary normative framework”, 41(2), *IIC* 2010, 187.

11. See the literature quoted in Pessach *supra*.

restrained in the public sphere; they are rather “discrete documents that operate with internal cohesion more than external linkages”<sup>12</sup>. Books, as physical objects, are gatekeepers of this cohesion and comprehensiveness that belong essentially to literary works. Similarly, dramatic or musical works are normally internally coherent units whose intimate sense and meaning depends on the maintenance of this cohesion. This holds true for most of the works that are generated in an authorial context. To be sure, although works are dense units, they can be “fragmented” by use. For instance, parts of the work may be extracted and used in other works as quotation or as part of a compilation, while the content of a work may be abridged, summarised or even partially reused in different context. All these ways of fragmenting the original whole in which the work consists presuppose a creative effort on the side of the subsequent author. The fact that the latter can legitimately fragment the work only on condition that he spends his own creative effort is an empirical proof of what we have called the “density” of the work itself.

In the cyber-context, by contrast, works tend to be *fluid* units. Not only is the internal cohesion no longer externally sustained by physical supports, but, most importantly, it is disarticulated in the first place. This happens essentially at three levels. First, at a pure technical level, works in digital format are reduced to a sequence of ones and zeros which flows in packages that can be disaggregated and re-aggregated. The case of Torrent files is probably at the moment the best exemplification of this technical disaggregation of the work’s unity. Second, at the level of human perception, works are increasingly exploited on a piece-by-piece basis instead of in whole; for instance, fragments of films or of broadcasts are displayed on YouTube, single tracks or parts of larger musical works are downloaded from iTunes or from peer-to-peer networks and snippets of books and of articles appear in search engines or in digital libraries as response to search queries. These forms of exploitation change the way by which works are commonly used, and one may wonder whether all these fragments of works do not acquire a new economic significance per-se.<sup>13</sup> Third, each work or part thereof is virtually linked to any external entity and can be equally internalised by any other work *via* framing, cut-and-paste or remix. As it has been pointed out, books, once digitised, are no longer bound by “the paradigm of the physical paper tome” and, through the search engine technology, they become part of a “single liquid fabric of inter-

---

12. Siva Vaidhyanathan, *The googlization of everything (and why we should worry)*, California University Press, Berkeley 2011, p. 171.

13. As suggested by the Belgian case *Google Inc v Copiepresses SCRL*, Court of First Instance of Brussels, [2007] E.C.D.R. 5, discussed below.

connected words and ideas”<sup>14</sup>. This “fabric” contains virtually the entire works of humankind in all languages, and it is not limited to books but extends to images, sounds and films. Once these items are transplanted from the authorial context to the cyber context via mass digitisation, then the “real magic” can start: “each word in each book is cross-linked, clustered, cited, extracted, indexed, analyzed, annotated, remixed, reassembled and woven deeper into the culture than ever before. In the new world of books, every bit informs another; every page reads all the other pages. [...] Once a book has been integrated into the new expanded library by means of this linking, its text will no longer be separate from the text in other books”<sup>15</sup>. As a matter of fact, in the “single liquid fabric” containing virtually all works produced by the whole humanity in all forms and languages, everything can be linked to anything without opposing resistance.

As a result, the transplant from authorial context to cyber context, that is from a dense to a fluid context through mass digitisation may bring about an unprecedented, and so far almost unnoticed, threat to author’s moral rights. As Hector MacQueen has pointed out, in the context of the latter developments of the digital world as determined by the advent of mass digitisation, “moral rights of attribution and integrity can be the bulwark of other authorial interests, offset by appropriately framed exceptions for education, research, news reporting, public libraries and parodies”<sup>16</sup>. In the following, we discuss how the right of integrity can help defining the legal boundaries of mass digitisation projects.

## Defining integrity

The right of integrity is commonly defined, in general, as the right to object to distortion, mutilation, or any other derogatory action in relation to the work which could be detrimental to the author’s honour and reputation.<sup>17</sup> Although referred to the honour and reputation of *the author*, the right applies to actions performed in relation to *the work*. To understand the proper meaning of the right of integrity it is essential to consider it from this particular angle.

Copyright subsists in what is generally called a “work”. Yet most of the rights that the law grants to the author of a work apply in fact to actions that third parties perform in relation to *copies* of the work. The author has in fact a right to make copies (reproduction), to issue copies to the public (publication) and to control

---

14. Kevin Kelly, “Scan this book!”, *The New York Times Magazine*, 14 April 2006, <[http://www.nytimes.com/2006/05/14/magazine/14publishing.html?\\_r=1](http://www.nytimes.com/2006/05/14/magazine/14publishing.html?_r=1)>.

15. *Id.*

16. Hector MacQueen “The Google book settlement”, 40(3) *IIC*, 247 (2009), p. 249.

17. See Berne Convention, art. 6 *bis*.

the circulation of copies (distribution). The rights of reproduction, publication and distribution represent undisputedly the pith and marrow of the author's economic rights and they are recognised as exclusive rights in all copyright systems. In certain jurisdictions the author has also the inalienable rights to have the copies effectively and efficiently disseminated (divulcation) and to remove the copies from the public sphere (withdrawal)<sup>18</sup>. All these rights enable the author to sue third parties for actions that they might perform in relation to *copies* of his work. They are copy-rights in a literal sense.

However, copyright does not enable control over copies only. So, for instance, the reproduction right is infringed not only when copies – namely “specimen of the same work”<sup>19</sup> – are made without authorisation. In fact, also non-literal and non-exact reproductions may be infringing. Here the infringing action is addressed to the work and not only to the copy as such. More precisely, the action is infringing to the extent that the *form* of the work is substantially taken, and not only the content or the matter expressed. The right of the author extends in fact to the form in which the work is expressed. The concept of form is broad enough to include “external” and “internal” form, the first being the sequence of words or of sounds or the arrangement of colours and figures by which the work is composed, and the latter being the construction of the expression in a broad sense, including the style and manner applied to that particular matter<sup>20</sup>. This means that any modification, alteration or adaptation of the form of the work is also restricted to the author. Translation of a literary work in a different language, for instance, is at the same time the creation of a new work and the alteration of the external form of the original work.

The right of integrity is closely related to the right to modify the work, that is to make translations, adaptations, arrangements or, as in the American wording, “derivative” works – however, it does not merge with it. Modifying the work is only a condition, and not even a necessary condition, for breaching the work's integrity. So, while an unauthorised translation impinges upon the right to trans-

---

18. The right of divulgation is recognised, in different forms, in Germany and in Italy; the right to withdraw or retract is recognised in France, Germany, Greece, Italy, Portugal and Spain.

19. Oxford English Dictionary, entry “copy”.

20. The distinction between internal and external form has been introduced by Joseph Kohler (1849-1919) on the basis of the classical argument developed by Johann Gottlieb Fichte in its 1793 essay “Proof of the unlawfulness of reprinting” (now available from *Primary Sources on Copyright (1450-1900)*, eds Lionel Bently & Martin Kretschmer, [www.copyrighthistory.org](http://www.copyrighthistory.org).) On the concept of form in copyright law see Maurizio Borghi, “Owning form, sharing content: natural-right copyright and digital environment”, in Fiona MacMillan (ed.) *New Directions in Copyright Law*, vol. 5, Elgar 2007.

late the work, a bad translation may infringe the right of integrity regardless of whether it is authorised or not. The two claims of infringement are clearly distinct. Moreover, integrity can be infringed by placing the entire work in an inappropriate context, without even modifying or mutilating the work as such. The scope of application of the integrity right is broader than that of the right to modify the work. Similarly, the integrity right is broader than the right of reproduction as applied to non-literal reproductions. Both modification and reproduction rights are in fact limited to the *form* of the work. The integrity right does not apply only to actions carried out in relation to the work's form. In a way, it can be infringed by any action performed in relation to the work itself.

Work as such	Work's form (both 'external' and 'internal')	Work's content	Copy of the work
Integrity	<ul style="list-style-type: none"> <li>• Reproduction (non-literal)</li> <li>• Adaptations, translations, etc.</li> </ul>	No copyright	<ul style="list-style-type: none"> <li>• Reproduction (literal)</li> <li>• Publication</li> <li>• Distribution</li> <li>• Divulcation</li> <li>• Withdrawal</li> </ul>

While copyright as such subsists in what is generally called a “work”, the right of integrity puts the work itself at the forefront. Yet what is a copyright “work”? In spite of the centrality of the notion of work in all copyright systems, one can hardly find a definition of the work in either statutes or case law<sup>21</sup>. It is generally known that in the civil law tradition the work is seen more as an act of one's own personality rather than an intangible object of property. This explains the existence of certain rights in relation to the work that are not at full disposal of the author, or that are simply inalienable. The notion of the work as an act instead as an object of property is rooted back in Kant's philosophy of right and his understanding of the “book” as a *public speech*<sup>22</sup>. As an object vested with certain rights, the work is essentially an act of communication between human beings, namely a speech addressed by an author to the public by means of a publisher. The latter is thus the mandatory of an act of speech over which the author maintains all rights and responsibilities. The right of integrity flows naturally from this understand-

21. See Brad Sherman, “What is a copyright work?” 12 *Theoretical Inquires in Law* (2011).

22. See Immanuel Kant, *Die metaphysik der sitten. Rechtslehre* [The Metaphysics of Morals. Doctrine of Right], in 8 Werkausgabe Immanuel Kant 404 (Wilhelm Weischedel ed., 1968) (discussion under heading “What Is a Book?”). Kant addressed the issue of unauthorized reprint also in the 1785 essay *On the Unlawfulness of Book Reprinting*. See Immanuel Kant, *On the Unlawfulness of Reprinting* (1875), now available from Primary Sources on Copyright (1450-1900) (Lionel Bently & Martin Kretschmer eds., 2008), <<http://www.copyrighthistory.org>>.

ing of the work as an inalienable act of speech, since distorting, mutilating or derogatorily treating a work is in a way the same as abusing one's own words.

From the stand point of the work as an object of property, the justification of the integrity right is not so straightforward. In particular, it is not clear why such right should be inalienable. Through the lenses of the utilitarian doctrine, in general, the fact that certain rights are inalienable is just a bizarre nonsense, since it would be in the interests of the author himself to have full disposal over the whole range of his rights. For instance, a "ghost writer" may monetise his voluntary status of "ghost" by transferring his paternity right to a third party; similarly, an author can allow any mutilations of his work upon payment. Yet the notion of the work as an act of communication between the author and the public provides a better understanding of the integrity right in its full meaning. This right does not simply reflect the author's self-interest in maximising the exploitation of his works. As a matter of fact, integrity is not even an author's interest only. It is rather, at the same time, in the interest of the public at large as well to have the words of the author addressed in a proper and comprehensive way. In Kant's terms, there is "a right of the public to a transaction with the author" which mirrors the right of the author to communicate his own thoughts to the public by means of publication. On this basis, it is reasonable that the right on work's integrity does not exhaust with the death of the author, nor it expires once the work falls in the public domain.

### Integrity and mass digitisation

From a legal point of view, the conversion of a work to a different format and its inclusion into a different context does not justify an alteration of the rights that apply to the work itself. This means that rights are neither expanded nor shrunk by modification of the form and context. For example, the Public Domain Charter of the Europeana makes clear that digitisation of content in public domain does not create new rights in it<sup>23</sup>. At the same time, digitisation does not shrink existing economic or moral rights. So, for instance, the same standard of integrity should apply when works are transplanted from "authorial" to "cyber" context, i.e. from physical to digital format. This point has been made in *Pink Floyd v EMI*, a UK case on the use of musical works originally recorded on physical support and subsequently exploited piece-by-piece as digital files and as ringtones. The High Court faced the problem of whether a contractual clause whereby the record label agreed not to sell physical albums of the rock band Pink Floyd "in any form other than as the current albums" and to exploit them "in exactly the same

---

23. <<http://www.europeana-libraries.eu/web/europeana-project/publications/>>.

form” applied also to online digital distribution of the albums. The Court, observing that the clause had the undisputed purpose “to preserve the artistic integrity of the album”, stated that “that purpose is as relevant to online distribution as to the sale of physical product”. As a consequence, the record label had a duty “to treat online distribution so far as possible the same way as the exploitation of the physical product”, and this duty was contravened by the selling of single tracks of the albums on streaming modality and of parts of tracks as ringtones.

The fragmentation of the work into separate pieces is one of the activities that potentially abridge the right of integrity in the cyber context. As far as mass digitisation projects are concerned, there are four main activities that may affect the work’s integrity. These are, in order of complexity: digitisation, indexing, search and automatic association.

### ***Digitisation***

The conversion of a work into digital format leads inevitably to a more or less visible loss of quality, depending on the type of the work and on the technology used to digitise. A first straightforward issue is whether, and to what extent, such a loss amounts to an abridgment of the work’s integrity. It must be observed that reproducing a work in lower quality does not per se amount to breach of integrity. For instance, reproduction of visual works in smaller size has not been found infringing in UK<sup>24</sup>. Similarly, the use of reduced size photographs as “thumbnails” in search engines has been considered to produce a “minimal loss of integrity” which does not pre-empt the finding of fair use in the US<sup>25</sup>. In a case on mobile ringtones, the German Supreme Court ruled that modifications due to the needs of technology do not violate the integrity of a musical works when the author has given his consent to that particular use<sup>26</sup>. One can safely assume that the loss of quality which can be reasonably expected by the use of a particular reproduction technology does not amount to breach of integrity.

However, digitisation is not just a technology to “reproduce” works. It is also, and more important, a technology to make works usable in a certain way. Take the example of digitisation of books in mass digital projects. Here digitisation implies two distinct operations. First, the book is “scanned”, namely it is reproduced and converted into a series of digital images. Second, the digital images are processed by optical character recognition (OCR) software, which converts the image into

---

24. *Tidy v Natural History Museum Trustees*, [1995] 37 IPR 501.

25. *Kelly v. Arriba Soft Corporation*, 336 F.3d 811(CA9 2003).

26. BGH 18 Dec 2008, I ZR 23/06. Mira, pp. 357-361.



a text file<sup>27</sup>. The first operation creates a *copy* of the work, same as with other reproduction technologies, such as photography and reprography – the only difference being that the image can be displayed on screens and copied in hard drives. Here the integrity of the work may be violated only when the loss of quality is not imputable to the technology as such, or when the book page is not entirely or truthfully reproduced, or when watermarks such as the brand of the digital project are superimposed to the image<sup>28</sup>. The second operation, *i.e.* OCRing, is qualitatively different than mere reproduction. Its purpose is not to reproduce the work, but to make the copy readable by computers. Through ORing, an object which can be read (only) by humans is turned into a machine-readable entity, and the work can be processed by software. This processing enables operations that are qualitatively different than those of “perceiving” the work itself, such as reading the book, viewing the image or listening to the music track or ringtone. Examples of automated processing that normally follow scanning and OCRing of texts are the extraction of information in order to index the work and the making of the text at disposal of users for search on a word-by-word basis and for search of terms in context.

While scanning *per se* may only amount to loss of integrity in exceptional circumstances – namely when the loss of quality is not justified by technological necessity – OCRing creates the conditions for systematic breach of work’s integrity by means automated processing. We consider these operations in the following.

### ***Indexing***

To index a digitised work means to provide the work with metadata to facilitate its identification and retrieval by search engines. Although this operation can be done manually, it is now increasingly performed with the aid of software that extracts information automatically not only from texts, but also from images and sounds. Indexing content is the key operation of search engines and it is preliminary of any use of digitised content in digital libraries and repositories.

It is a well established principle that indexing and creating indexes of copyright works do not generally amount to copyright infringement nor to infringement of author’s moral rights. In a French case of the pre-digital era, the Court de Cassation ruled that the indexing of journal articles by selection of keywords and the making of short *résumés* does not infringe copyright in the articles and does violate their integrity, insofar as these activities are functional to a “purely in-

---

27. See *Infopaq International A/S v Danske Dagblades Forening*, Case C-5/08 [2009] E.C.D.R. 16, § 18-19.

28. This example has been discussed in Adolf Dietz “Authenticity of authorship and work” 165 (Copyright in cyberspace, ALAI Study Days 1997).

formative” purpose and represent “the expression of free choice of the author of the secondary work”<sup>29</sup>. It is important to note that the “free choice” of the subsequent author – that is, the author of the index – must be clearly recognised in the expressive form of the index itself, namely in the selection of keywords and in the composition of *résumés*. Failing this element, the index may not be an independent work of authorship but may unduly overlap with the indexed work. For instance, the selection of keywords could be perceived as an “objective fact”, and the *résumé* may be understood as expressing the view of the author of the indexed work. By contrast, both the keywords and the *résumés* are the outcome of a choice which may – but does not have to – coincide with the intended purpose of the original work.

Moreover, according to the French court, the index must be “purely informative”, that is it must have the sole purpose of informing the public about the existence of a certain work. It has not to replace the original work in any way<sup>30</sup>.

The combination of these two elements – the “informative” and the “free choice” element – provides a good set of criteria to test whether indexing in mass digitisation projects violates the work’s integrity. The problem that might arise is when metadata on books and on other content are too poor or too inaccurate to properly identify the work, or are such that the work is systematically identified in an improper way<sup>31</sup>. This problem is further enhanced when metadata are not created by some expenditure of independent skill and judgement, but are automatically generated via data mining on books or on other content. Is there still an element of “free choice” in the way by which the indexed works are presented? And if not, how does one have to classify, from a copyright perspective, the relationship between the index and the indexed work? This question is particularly relevant when referred to the activity that is commonly associated with indexing in mass digitisation projects, namely searching.

## Search

Once digitised and indexed, works are available for searching within search engines. As discussed earlier, in the example of books searching is made possible by OCRing, a process by virtue of which printed pages become searchable “inside”, that is on a word-by-word basis. This processing of the book’s pages does

---

29. *Le Monde c. Microfor*, Cour de Cassation, 30 Octobre 1987, 86-11918.

30. See also *Ty Inc. v Publications International Ltd*, 292 F.3d 512 (7th Cir. 2002) (distinction between “complementary” and “substitutional” copying in the fair use analysis).

31. For a detailed analysis of Google Book’s metadata see Geoffrey Nunberg “Google books: a metadata train wreck” <<http://languageolog.ldc.upenn.edu/nll/?p=1701>>.

not represent *per se* a violation of the integrity of the work which is fixed in the printed medium. This is because, as a technical operation, OCRing modifies only the format in which the work is fixed but does not touch upon the work's form or even the work as such. Modifications that are technically necessary in this respect do not amount to infringement of moral rights. Nevertheless, OCRing creates the *conditions* for possible violations of integrity on a large scale. The case of Google Books is illustrative of this situation. Here books and other literary works are digitised and made searchable by users, which can search inside books on a word-by-word basis and view short excerpts or "snippets" in response of their queries. By entering a search query, subject to display are excerpts from a book that contain that particular word or string of words. Moreover, excerpts are displayed alongside excerpts from other books that contain the same word or string. And this is not the only case. The large corpus of digitised books is at the same time integral part of the large Google's database which include web pages, news, geographical locations and virtually all "world's information"<sup>32</sup>. This means that excerpts from a book are made available not only to users that search inside that particular book, and not even only to users that search into the corpus of Google Books, but to any user who enter a search query in the Google search engine, and those excerpts are displayed alongside excerpts from any other web resource<sup>33</sup>. Accordingly, every search query generates automatically a fragment of the work which in turn is presented in a context which is determined by the algorithm of the search engine. Is there in this practice violation of integrity?

In Europe, two courts responded in the affirmative<sup>34</sup>. In *Google v Copiepresse*, the Belgian Court of first instance of Brussels faced the problem of whether the service Google News, which provides internet users with an automatic selection of news items from the web servers of the written press, infringes copyright in newspapers articles. *Inter alia* the court examined the closely related issues of the applicability of the exception for quotations and of the infringement of the moral right of integrity. As to the first point, the court correctly argued that under Belgian law – but similar finding should be made in most European jurisdic-

---

32. As it is well known, the Google's corporate mission is to "organize the world's information and make it universally accessible and useful" (<<http://www.google.com/corporate>>).

33. It can be observed, incidentally, that books forming the corpus of Google Books are only available to Google search engine, and do not feature in the results of other search engines like Yahoo! or Bing.

34. *Google Inc v Copiepresse SCRL*, Court of First Instance of Brussels, [2007] E.C.D.R. 5; *Editions du Seuil et autres c. Google Inc et France*, Tribunal de grande instance de Paris 3ème chambre, 2ème section Jugement du 18 Décembre 2009.

tions<sup>35</sup> – the “right to quotation” does not apply when excerpts of works are extracted and grouped automatically, without human intervention<sup>36</sup>. To the court, a “quotation” is meant to be used in a subsequent work to illustrate a proposition or defend an opinion; by contrast, Google “does no more than incorporate the ‘quotations’ and owes its substance solely to the extracts of works reproduced, which is contrary to the spirit of the right to quotation”<sup>37</sup>. Given that Google’s excerpts are not “quotations”, their automatic extraction and grouping may violate the integrity of the work. In this respect, Google contended that there is no damage to “the integrity of the work where the quotation of a text is to be found with another quoted text or photos” in that “the internet user knows very well that it is dealing with a quotation, and sees the original text each time in its original context by clicking on a hyperlink”<sup>38</sup>. The court disagreed and observed that “the circumstance that the internet user is aware that it is only dealing with a fragment of the work does not seem relevant in relation to respect for the integrity of the work.” This is because “Google groups the different extracts of articles, which can originate from any source, by theme, so that *the editorial or philosophical approach espoused by the author may be altered*”<sup>39</sup>.

This conclusion can easily apply to mass digitisation projects, and in particular to projects like Google Books where the digitised works form part of larger search engines databases. This is confirmed by the French decision in *Editions du Seuil c. Google France*, where the court found that “the display of excerpts from works that

---

35. The exception for quotations is harmonised by art. 5(3)(d) of the Directive 2001/29/EC, which reads: “Member States may provide for exceptions or limitations to the rights provided for in Articles 2 [Reproduction] and 3 [Communication to the public] in the following cases:

[...]

(d) quotations for purposes such as criticism or review, provided that they relate to a work or other subject-matter which has already been lawfully made available to the public, that, unless this turns out to be impossible, the source, including the author’s name, is indicated, and that their use is in accordance with fair practice, and to the extent required by the specific purpose.”

The exception for quotations is not enacted in the Czech Republic and in Slovenia. In Ireland and the UK there is no express mention to quotes and the quotation exception falls under fair dealing for criticism and research.

36. *Google v Copiepresse*, § 130.

37. *Google v Copiepresse*, § 131. In *Editions du Seuil c. Google* the French court affirmed that the exception for “short quotations” (Code de la Propriété Intellectuelle, art. L. 122-5) cannot apply to the display of snippets in Google Books.

38. *Id.* § 159.

39. *Id.* §§ 160-161 (emphasis added).

Google Inc. recognises to be truncated randomly and in form of ripped banner of paper undermine the integrity of the works"<sup>40</sup>. In the context of mass digitisation projects like Google Books, works are increasingly exposed to the possibility of being associated with, or even linked to, content originating from different sources. Such automatic association creates further conditions for abridgement of integrity.

### ***Automatic association***

As seen in *Copiepresse*, integrity is violated when the work is displayed in contexts where the "editorial or philosophical approach espoused by the author" is altered. It is a well established principle that the author has a right to object publication or republication of his work in contexts that do not fit the intended purpose of the work. In the USA as well, where the moral right of integrity is not codified, the contributor of a collective work has a right not to have his work republished separately or in other collective works that do not belong to "the same series"<sup>41</sup>. Although the rationale of this norm is to protect the economic interest of the author, the result is that the author can object any alteration of the context in which the work is published.

In case of mass digitisation projects, works are *de facto* republished in contexts where the original editorial approach cannot be easily reproduced. Here again a distinction must be made between what is technologically necessary and what exceed this necessity. A digital library is by definition an environment which is different than any context in which works as such or physical copies thereof are normally accessed, such as galleries or libraries<sup>42</sup>. This, however, does not exempt digital repositories from a duty to present works in an environment which respects the editorial and philosophical approach of the work itself.

The typical case in which integrity of the work may be violated is that of "bad association", namely when a work is associated with other information in a derogatory way. For instance, a book containing explicit language or an art photograph of a nude model could be automatically presented in connection with pornographic content or linked to information which has nothing to do with the book or of the photograph. The fact that these associations are generated automatically, that is without human intervention, does not mean that there cannot be violation of the work's integrity. In recent cases on search engines, French and

---

40. *Editions du Seuil c. Google*.

41. 17 U.S.C. § 201(c). See *New York Times Co. v Tasini*, 533 U. S. (2001).

42. For a discussion of the difference between libraries and digital libraries in the context of user's privacy see Elisabeth A. Jones & Joseph W. Janes, "Anonymity in a world of digital books: Google books, privacy, and the freedom to read", 2(4) *Policy & Internet*, 43 (2010).

Italian courts have found that associations generated by Google's "autocomplete"<sup>43</sup> are capable of determining defamation<sup>44</sup>.

More generally, mass digitisation projects present works in "reading environments" that are increasingly shaped by automatically generated associations. While the fact of associating works with other works is a natural one, and it is the principle upon which libraries are made, its implementation by digital technology may lead to drawbacks. As put forward in an opposition to the Google Books Settlement Agreement, the systematic lack of human control may cause works to be "associated with authors' work in ways that are objectionable, offensive, or harmful to the author"<sup>45</sup>. For example, automatic associations may be generated as effect of "groups attempting to create a false appearance of endorsement"<sup>46</sup>. More subtly, behaviours of groups of readers which use an author's work for own purposes, for instance to support own political views, may influence algorithms so that the author will be automatically associated with those views. Moreover, computational analysis on corpuses of millions of books and of other digitised works, coupled with aggregated data mining, are able to associate an author with other authors, information, products, or even "ideas" independently from their expression. For instance, a book may be displayed alongside a list of "key ideas" as extracted via automatic text processing, and the reader may be re-addressed to authors that allegedly share "similar ideas" based on associative and taxonomic data analysis<sup>47</sup>. A range of "proxies" can be associated with works, spanning from snippets, quotes, cross-referencing or even "key ideas". Are all these associations, which potentially violate the work's integrity, justified by the "technological necessity" of transplanting a work from physical format to the digital environment?

A critical issue is whether association with advertisements is generally compatible with the "editorial and philosophical" approach of works that are hosted by a digital library. In commercial digitisation projects, "discrete advertisement" may be dis-

---

43. On the functioning of Autocomplete see <<http://www.google.com/support/websearch/bin/answer.py?answer=106230>>.

44. M. X... /Google Inc., Eric S. et Google France, TGI Paris 17ème chambre, 8 septembre 2010; Mme C. / Google France et Inc., TGI Montpellier, 28 octobre 2010; Tribunale di Milano, ordinanza 31 marzo 2011.

45. Objections of Arlo Guthrie, Julia Wright, Catherine Ryan Hyde, and Eugene Linden to Proposed Class Action Settlement Agreement, *Author's Guild, Inc. v Google, Inc.*, No. 1:05-CV-08136 (2 September 2009), p. 12.

46. Id.

47. See Bill N. Schilit & Okan Kolak "Exploring a Digital Library through Key Ideas", Proceedings of the 8th ACM/IEEE-CS Joint Conference on Digital Libraries (Pittsburgh, Pennsylvania, USA, June 16-20, 2008), available at <http://sites.google.com/site/schilit2/fp035-schilit.pdf>.

played in connection with books or articles. This may be in contrast with the editorial approach that underlies most of the works that are hosted by the service. It is no accident if advertisement is normally not included in book's pages, or if scientific journals who host advertisement pay particular attention not to place it alongside articles. These are forms of respect for the work that are deeply rooted in the publishing practice, and any alteration of these forms which exceed what is technologically necessary to digitise the work is a potential threat to the integrity of the work.

## Conclusion

Mass digitisation has become paramount in the online world as the activity by which the cultural heritage of humankind is digitised in bulk to form part of the collection of online archives, repositories and digital libraries. While most of the rights pertaining to the digitised works, and particularly the economic rights, may be expired, certain moral rights are perpetually in force in most European jurisdictions. As we have seen, the moral right of integrity does not merely protect an author's interest, but is representative of a more general interest of the public at large. As a matter of fact, it is in the interest of the whole society to preserve the integrity of works that form part of our cultural heritage, and in this respect the integrity right can be seen as a bulwark of other more fundamental societal interests. If this is the case, then the question arises as to whether, and by which means, integrity is threatened by mass digitisation.

It has been rightly observed that rights are technology neutral, and violations of moral rights must be determined in similar way irrespective of whether they are performed with digital or analogue technologies<sup>48</sup>. Similarly, the rights pertaining to works are not altered when they are transplanted from the analogue to digital environment. However, mass digitisation projects brings about a technological shift in the way in which works of authorship are used: works are no longer dealt with with human intervention only, but are increasingly subject to automated processing. Such processing inevitably modifies both the work itself and the context in which the work is displayed to the public. Not all modifications introduced by automated processing of works are as apparent as those that occur by means of human intervention. Still, they are all but irrelevant. In particular, they are not all justifiable on technological grounds. Here again, the legal challenge is to draw a distinction between modifications that are "technologically necessary" and modifications that exceed technological necessity.

---

48. Salokannel & Strowel, *id.*, p. 206.

# **From theory to practice: autonomy, privacy and the ethical assessment of ICT**

---

---

**William Bülow & Misse Wester**

---

---

## **1. Introduction**

The ethical issues in relation to new developments in information and communication technology (ICT) are often framed in terms of privacy (e.g. van den Hoven 2009; Rössler 2005; Nissenbaum 1998). Privacy is held to be an important value in western democracies, and it is argued that having a private sphere is a necessary condition for other democratic rights, such as liberty and integrity, and values such as autonomy (e.g. Rössler 2005).

However, due to developments in informational technology, large amounts of personal data are stored by different actors in society. While the phenomena of collecting personal data is not new, there are mainly two things that have changed in the past decade or so: first, more information is being collected than ever before and secondly, information is not just stored but is subjected to some sort of analysis (Lyon, 2006). Information about individuals is collected as they act in the normal course of their public lives. Information is shared in transactions with retailers, using credit card, mail order companies etc. The use of RFID-tags and CCTV cameras in various context, including workplace and public spheres, as well as the widespread use of e-services and internet helps to increase the amount of information stored about individuals by various actors. Also, the means of collecting and storing data has other consequences. While information is often collected by an individual, an agency or organisation with which a person interacts, information about individual can be collected by secondary users who acquire information from either primary or secondary sources (Nissenbaum 1998).

As various forms of information technology are emerging and being used in various parts of our personal and public lives, it has become important to consider the ethical aspects and the assessment of the possible use of these technologies. To achieve this end, one must identify how different sorts of information stored about individuals related to the issue of privacy. This paper highlights the complexity of informational privacy and its relation to autonomy and the ethical assessment various uses of information technology. It is argued that due to its connection to autonomy, together with the ambiguous nature of referential



descriptions, the possible intrusions to privacy which a particular information technology may give rise to, are hard to assess. This implies that the use of ICT cannot be determined solely on the basis of what sort of information is collected. It must also consider whom the information is about, in what context it is given, for what purpose.

The paper proceeds as follows: In section 2 we will discuss the importance of privacy and its connection to autonomy. In section 3 we will discuss what sort of information should be protected. In section 4 we present four scenarios from a survey study conducted in Sweden 2010 and discuss how they relate to our overall argument. In the final section we sum up our conclusions.

## 2. The importance of privacy

Privacy is held to be important because of its connection to autonomy (e.g. Rössler 2005; Palm 2009). Protection of a person's privacy enables her to control the access to information, how it is distributed and to whom, and is a precondition for leading an autonomous life. For instance, Rössler (2005) argues that "privacy protects autonomy in those respects in which the exercise of autonomy is dependent upon my control of the access of others to me, to my person, to my (reflections on) decisions and to information about me" (Rössler 2005: 73). Similarly, Palm (2009) suggests that a "failure to protect privacy is problematic for the reason that we thereby fail to secure the more fundamental value of autonomy" (Palm 2009: 240). On this view, if one desires to live one's life as an open book, one should be able to do so, and whether one want to restrict the access to different sorts of information, this should be respected. In either case, the protection of privacy entails that a person should be able to control information, as well as private areas (such as ones home) from the unwanted intrusion of others.

Seeing privacy as a precondition of autonomy, intrusions to a person's privacy is problematic because it limits or restricts that person's autonomy. The amount of information people have about a person often affects how that person will behave towards those people. People act upon certain expectations about the particular situation in which we act. Rössler (2005) uses the following example as an illustration: in the case of hidden video surveillance in public places persons have certain expectations concerning unfamiliar people whom they meet and have expectations on how they will behave. However, persons do not expect being recorded on film and thus being converted into something that can be used reproduced and shown in public irrespectively of time and place (Rössler 2005). If the person being recorded by hidden surveillance cameras knew of this, this person would possibly behave differently. On this view, the violation of the right to privacy is a violation to the person's autonomy. Also, characterizing violation

of the right to privacy as a violation to the person's autonomy also shows how the case of hidden video surveillance would be a violation to autonomy even though the person is not aware of being filmed. For even though a person's behavior in public is self-determent, this behavior is only apparently so because it was made by the person under false assumptions (Rössler 2005).

Of course there are other reasons why a person might want to keep certain information privacy. Most straightforwardly, the protection of privacy helps to prevent various sorts of harm, including reputational harm and the risk of being victim for cybercrimes. As van den Hoven (2008) points out, certain harms cannot be inflicted (or at least not easily) if certain information was not available, such as identity theft and stalking, and is in favour of the protection of personal data. However, despite that personal information is protected, the respect for personal autonomy implies that a certain form of surveillance can be problematic anyway. Moreover, as large amounts of personal information are stored about various actors, individuals are continually giving up the control over their personal information. This may, as Rössler points out, come to limit their autonomy:

If it can in principle no longer be taken for granted that one has control over one's informational self-determination or that one is not (constantly) being observed, and if, as a result, one must (constantly) present oneself as though one were being observed, the result is a loss of autonomy in terms of the authenticity of one's behaviour, which is turned into behaviour *as if*, that is alienated behaviour (Rössler 2005: 128-9).

Following the idea that the protection of privacy is a precondition of autonomy, we will now discuss some issues which may arise when assessing possible uses of ICT.

### **3. Which information should be protected?**

In addition to its account of the value of privacy, a normative theory of privacy must be able to account for what sort of personal data should be worth protecting. In a series of papers, philosopher Helen Nissenbaum has argued that information technologies raise new privacy issues which are seldom acknowledged by philosophical accounts of privacy. Information about individuals is collected as they act in the normal course of their public lives. Information is shared in transactions with retailers when using credit card or when using mail order companies. In addition, the new means of collecting and storing data involves another layer of surveillance that builds upon them. While information is often collected by an individual, agency or organisation which whom a person interacts, this new layer of surveillance involves a new category of users who acquire information from either primary or secondary sources (Nissenbaum 1998). While we do share this information freely it is possible to combine various sources based on personal data, consumer preferences, habits etc and it is possible to create a pretty good picture of an individual by combining various sources. This, Nissenbaum refers

to as the problem of privacy in the public (e.g. 1998; 2004). While this is not conceived as classical instances of violation to privacy, Nissenbaum suggests that it is problematic because the aggregation of personal data can be harmful to personal integrity. Another issue is that even if individuals willingly share one set of information in one context, she might want to avoid access to it in another (Nissenbaum 1998).

Part of the problem which Nissenbaum aims to capture is that certain information, when shared in one context, may be unproblematic while being harmful when shared in another context of put together with other personal information. A similar point is illustrated when recognizing a basic ambiguity about descriptions. As, van den Hoven (2008) points out, it is possible to distinguish *attributory* and *referential* descriptions. “The young man who takes the metro every weekday 08 am” could have more than one individual satisfying the description and is an instance of attributory description. However, at the same time, “the young man who takes the metro every weekday 08 am” can be used referentially, when we have a particular person in mind. It is important to note that both attributory and referential descriptions figure in epistemic and doxastic strategies to collect information on people, and are directly or indirectly related to expanding our knowledge about them. In other words, they are both *identity-relevant information* (van den Hoven 2008).

As van den Hoven points out, the distinction between referential and attributory descriptions is important since much data that is collected through various ICT, such as RFID-technology and CCTV cameras do collect data which in itself is attributory. It is therefore troublesome that only referential information should be protected. Moor (2008) points out, that as technological revolution increase their social impacts, ethical problems will also increase. This, Moor argues, is not simply because more people are affected, but because inevitably, revolutionary technology will provide numerous opportunities for actions. Information technology is clearly such a technology, enabling individuals, organizations, governments and governmental agencies to gather and store large amounts of personal data. While the importance privacy issues have been discussed before the widespread use of information technology (e.g. Rachels 1975), the privacy issues in relation to ICT are different, mainly because they enable information to be collected in one context, stored and sooner reproduced in another and even combined.

Another problem with assessing which sort of information should be protected arises directly from the importance of privacy and its connection to autonomy. What is and what is not private information differs among individuals and different sorts of information may be perceived as private by certain individuals while not to others. For instance, it is important to a Muslim woman not to show her

hair and at time, hair is not a private matter to a Swedish woman. In a similar vein, protection of privacy as a precondition to autonomy implies that whatever information that relates, or can relate to an individuals' autonomy, that individual desires to hold this information private, or as Rössler (2005) puts it:

Not only should what a person divulges not find its way into the wrong context, but what she never wants to divulge in the first place should remain what it is – a private matter. The seclusion or secrecy into which she can withdraw represents a limit to any social relationship in which she finds herself, for in all such relationships she is entitled to informational privacy of this order, and this ultimate control over her self-presentation constitutes the condition for her autonomy. This is, on the one hand, because subjective chaos of thoughts, feelings, images, self-definitions and self-interpretations is constitutive in determining what discloses itself as essential to person's life and how it does so (Rössler 2005: 140).

While it may seem like an attractive conclusion, it is in fact dubious. Despite how much a person divulges certain information about oneself there may be other reasons, such as public safety, for which this information must be shared anyhow. However, as autonomy is the sacred value for which privacy must be protected, one must assume that almost any sort of information might be held to be private, not because it is of a certain class, but because it relates to a particular individuals self-determination.

Clearly, an ethical assessment of ICT must answer questions about what aspects of personal autonomy will be restricted and how likely would it be that personal autonomy is actually reduced (Rössler 2005). However, as this is mandatory, it ought to be clear that due to its connections to autonomy the possible risks to privacy poses by the use of ICT cannot be determined solely on the basis of what sort of information is collected. It must also consider whom the information is about, in what context it is given, for what purpose etc, i.e. an ethical assessment of ICT, such as surveillance cameras or the use of RFID-tags in passports, should be more context-sensitive. It remains, however, to be discussed how such a model for evaluation would look like.

As the ethical assessment of ICT should be context relative, we will now illustrate how acceptance of ICT is also dependent on various factors.

#### **4. Acceptance of various ICT solutions**

In order to illustrate perception and acceptance of ICT we present empirical data from a survey study distributed among a representative sample of the Swedish population from 2010. Here two technologies used for collecting personal data are selected, the use of positioning technologies in mobile phones and the use of RFID tags. These technologies each have two versions, and can be summarized in the following way:

RFID tags are used for two purposes, where the first is for public transportation where information about your travel routines are stored by your local transport provider. In the second scenario, RFID tags are used for tracking shipments with e.g., clothes. Once the clothes have reached the retailers, the RFID tag remains in the individual article of clothing where it can be scanned by other retailers and used for marketing purposes.

The second technology deals with global positioning systems (GPS) available in mobile phones. In this scenario two different versions were used to measure public acceptance, where the first was the possibility to use the GPS system to share your location over the Internet so that friends and family could track an individual's movements and this information is shared on a voluntary basis by the person herself; in the second, the police can under specific circumstances activate this function in order to track individuals without their consent. In these cases, the same technology is used and collects the same sort of information. What is different is who collects it and whether the individual do consent.

Overall, the results show these two technologies regardless of application are not widely desired by the public. However, as the sort of information is similar in all cases, there are differences in acceptance. The acceptance for the commercial use of RFID tags are seen as most privacy invasive and positioning by police authorities as least invasive. This implies that the purpose of gathering data matters to how technologies that are privacy invasive are perceived. The commercial use of RFID tags in clothes is seen as the most questionable and outrageous. However, most people would not do anything to avoid being subjected to these technologies – with the exception for RFID tags in clothes.

## 5. Conclusion

The protection of privacy is important because it is a precondition to personal autonomy and to control of information about ourselves is necessary in order to determine how we present ourselves in different contexts. However, as autonomy is a precondition for autonomy, it also gives rise to an epistemological problem when assessing the ethical acceptance of ICT. What is held to be private information to different individuals in different context. This, calls for more context sensitive evaluations of ICT when used in various parts of public life.

## References

- Etzioni, A. (1999). *The Limits of Privacy*, New York, Basic Books.
- Lyon, D. (2006). *Surveillance, power and everyday life*, *Oxford Handbook of Information and Communication Technologies*, Oxford University Press.
- Moor, J. (2008) "Why We Need Better Ethics for Emerging Technologies", in *Information Technology and Moral Philosophy*,(ed). van den Hoven, J and Weckert, J. Cambridge, Cambridge University Press.
- Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public, *Law and Philosophy*, 17, 559-596.
- Nissenbaum, H. (2004). Privacy as Contextual Integrity, *Washington Law Review*, 79, 119-157.
- Palm, E. (2009). "Securing privacy at work: the importance of contextualized consent", *Ethics and Information Technology* 11: 233-241.
- Rössler, B. (2005). *The Value of Privacy*, Cambridge, Polity Press.
- van den Hoven, J. (2010). "Information Technology, Privacy and the Protection of Personal Data", in *Information Technology and Moral Philosophy*,(ed). van den Hoven, J and Weckert, J. Cambridge, Cambridge University Press.

# **Evolution of data protection starting from the French experiment, in a context of vicinity: solutions and new questions - prospects**

---

---

**Georges Chatillon**

---

---

The French CNIL (National Commission for Data-processing and Freedoms)

In figures:

Each year:

- 72.000 declared treatments
- 120.000 phone calls
- 25.000 received mails
- 5.000 complaints or requests for advice
- 200 controls
- 13 millions of €: budget

The French law of 1979, data-processing - files and freedoms instituted an prior agreement of the CNIL when the administration wanted to carry out an automated treatment of personal data. Recently, at the time of a dinner in which I took part, with the invitation of the chairman of the SNCF, Alex Türk, president of the CNIL, pointed out with the assistance that, between 1979 and 2004, date of the transposition of the European directive, the CNIL had never given unfavorable opinion.

The law of 2004 institutes a control a posteriori of the legality of the automated treatments of data, at the same time for the public administrations and the private sector. Since 2004, the CNIL carries out effective thorough controls, as we will see it.

Since the years 1980, the CNIL used its Internet site for “to communicate” and to make publicity. The Net surfers are invited to check, on line, in some clicks, which are the “traces” left by their computer at the time of connections Internet. In fact, all the technical data of the computer and navigation are directly visible and alert the Net surfer on the questions of protection of the personal data.

The CNIL knew to mitigate the chronic lack of financial means and administrative staff and control thanks to his legal status, its strategy, and five activities:

**Legal status**

It is an independent administrative authority

**Strategy**

CNIL is interested mainly in the daily problems of the people and the companies

**Priority activities**

- 1) CNIL is a contentious authority
- 2) It carries out spectacular controls giving place to publicity and modifications of the behaviors of the actors in the fields of his competence
- 3) It profits from the activity from the Correspondents Data-processing and Freedoms of growing number in the companies and the administrations
- 4) It develops relations followed and rich with the other CNIL in Europe and in the world
- 5) It takes part in work of the European Commissioner to the data protection and the Group Article 29

The CNIL appears, today, like a guard and a credible defender of the personal data and private life because it is illustrated in the majority of the fields of the daily life and thus it interests people.

However, successes of the CNIL are ``relative'' and nonsystematic for reasons of lack of means materials, manpower, of competence. In addition the passion for the social networks, Facebook, Twitter, etc. is a permanent provocation for the gendarme of the data protection since these same social networks do not respect the European right.

The offensive dynamism of the social networks causes contrasted reactions.

**To control and count the files**

The CNIL holds with the provision of the public the "file of the files", i.e. the list of the treatments which were declared to it and their main features.

For the treatments or files of the least dangerous personal data and most current, the CNIL works out text-frameworks to which the persons in charge of personal data must refer to carry out reduced declaratory formalities or in being exonerated.



The data processing at “the risks” or significant is subjected to authorization or opinion of the CNIL. The non-observance of these formalities by the persons in charge of files is liable to administrative or penal sanctions.

### ***1. The CNIL is a contentious authority***

Since the reform of the data-processing law and freedoms of August 6th, 2004, the CNIL can, at the conclusion of a contradictory procedure, decide to pronounce various measurements against the persons in charge of treatment who do not respect the law: a warning, an injunction, a pecuniary penalty which may reach 300.000 €, an injunction to cease the treatment, etc., For pronouncing these measurements, the CNIL sits in a specific training, made up of six members called “contentious formation”.

This authority meets at least once a month to decide measures to be taken with regard to the persons in charge of treatment who do not respect obviously the data-processing law and freedoms. The examined files make continuation generally with a mission of control carried out by the CNIL, with the reception of complaints or any situation in which the dialog did not make it possible to restore a situation in conformity on the legal level.

### ***2. To control - to sanction***

The actualization of the law of January 6th, 1978 by the law of August 6th, 2004 marked a strategic evolution of the activity of the CNIL and equipped it with new powers to control and sanction.

#### **2.1 Controls**

The power to control of the CNIL constitutes an average privileged mean of intervention near the persons in charge of personal data.

The CNIL apprehends the reality of the data processing thus personal and appreciates the consequences of the recourse to data processing in certain branches of industry.

The missions of control lie within the scope of an annual program of controls or in answer to specific needs (felt sorry for, requests, of council, new technology...).

The annual program of controls is adopted in plenary session. It is elaborated according to the topics of topicality and the problems whose CNIL is seized.

To control computer applications, the CNIL can:

- to reach all the professional buildings,

- to ask for communication of any required document and to take copy of it,
- to collect any useful information,
- to reach the computer programs and the data.

The CNIL in addition supervises the information system security by making sure that all the precautions are taken to prevent that the data are not deformed or are communicated to unauthorized people.

## 2.2 Sanctions

The CNIL has a large range of coercive measures and sanctions: except the warning, the CNIL can after an unfruitful injunction and at the conclusion of a contradictory procedure, to impose a pecuniary penalty, except for the treatments implemented by the State, an injunction to cease the treatment for those which concern the declaratory mode, or to withdraw an authorization.

In the event of urgency and of violation of the rights and freedoms resulting from the implementation of a treatment, the CNIL can decide the temporary interruption of this one or the locking of data (for three months) except for certain treatments of the State and in particular of the treatments known as of sovereignty interesting the state security, defense or public safety and those having for object the search for penal offenses or the execution of the judgments, for which the CNIL however has the possibility of informing the Prime Minister “so that it takes, if necessary, measurements making it possible to put an end to the noted violation”. In the event of gravely hurt and immediate with the rights and freedoms, the president of the CNIL can ask in summary procedure the judge to order any security measure necessary to the safeguard of these rights and freedoms.

In addition, a stop of the Council of State February 19th, 2008 recognizes with the CNIL in the exercise of its capacity of sanction the quality of court.

The amount of the pecuniary penalties likely to be inflicted can reach 150.000 euros at the time of the first noted failure and 300.000 euros or 5% of the sales turnover net of tax of the last exercise if it is about a company within the limit of 300.000 euros. The amount of these sanctions must moreover be “proportioned with the gravity of the made failures and the advantages drawn from this failure”. The penal sanctions envisaged in articles 226-16 to 226-24 of the Penal code can also apply, the CNIL having the possibility of denouncing with the Public prosecutor the infringements to the law of which it is informed.

### ***3. The Correspondents Data processing and Freedoms***

The data-processing correspondent and freedoms (DPFC) became an inevitable actor in the French landscape of the data protection: the designation of a DPFC within a company, an administration or an local government agency ensures the promotion of the data-processing culture and Freedoms.

#### **Last figures**

6869 organizations appointed a Data-processing Correspondent and Freedoms.

1803 correspondents are in activity

### ***4. The CNIL develops relations followed and rich with the other CNIL in Europe and in the world***

Vis-a-vis the Universalization of the exchanges of information (Internet, Google, social networks .....), with the successive waves of technological innovations, the new means deployed to reinforce the collective security of the people, (biometrics, videowatching, controls...) the CNIL engages actively with the international plan and European, while reinforcing his technical expertise.

#### **4.1 The question of the technical expertise is fundamental**

The capacity to include/understand and anticipate technological developments is from now on essential to the authorities of data protection.

The CNIL is requested more and more on the technological subjects and the implementation of innovating information systems (biometric passport, personal medical records...).

By advising the companies as of the design of their computing systems, the CNIL can encourage them to modify them, use alternative technical solutions or to envisage guarantees for the data protection of the people.

To accompany the technological mutations, the CNIL develops an activity of day before and expertise on the innovations, and reflection on the security questions which arise to the turning new technologies.

In this field, the priorities of action of the CNIL are:

- the development of the technical expertise concerning of the complex computer applications (like biometrics or architectures for the e-voting);
- the thorough evaluation of the safety of computing projects of national scale (as biometric visas or the passport, personal medical records or the electronic mobile bracelet);

- the participation, at the European or international level, work groups of data protection (Internet Task force of G29, International Working Group one Dated Protection in Telecommunications, group of expert);
- day before and the reflection upstream on the major technological subjects which will have to influence our company in the future, in particular the field of the nanotechnologies which will have an unquestionable impact on data-processing architectures and their relations with the individuals,
- the anticipation of the technological changes so that they hold account, as of their design, of the problems data processing and freedoms. This requires the development of bilateral relations with the major industrial actors and the implication, as a member of the consortium or the steering committee, in national or European research projects;
- the information of the citizens as well as the participation in conferences on the problems of technology, the safety and the data protection;
- the contribution to actions of standardization, in particular in the field of safety (for example while taking part in the committee of the general Reference frame of interworking, controlled by the Head office of the modernization of the State).

The innovation must remain compatible with an effective protection of the personal data and private life.

Let us quote, as example, some technological innovations supervised by the CNIL:

- Community search engines and sites
- Billboards bluetooth
- The geolocalization
- RFid
- Infotraffic
- Pay as you drive
- Streetview
- Biometrics
- Facial recognition
- Recognition of the venous network of the finger by Hitachi

## **4.2 The co-operation Police - Justice within the European framework and with the international scales**

The exchanges of information personal multiply within the framework of the European and international police co-operation, in particular since the attacks of September 11th, 2001 which resulted in a reinforcement of the security measures interior and control of the migratory flux.

Concretely, the Member States of the European Union can from now on exchange the genetic prints and digital certain people (treated of Prüm), while many international agreements authorize the transfer of new personal data within the framework of the fight anti-terrorist, against organized criminality or illegal immigration. In this context, the role of the controlling authorities created at the European level is paramount: the CNIL sits within the body independent of control Eurodac 2, at the sides of its counterparts and of the European Controller of the data protection, and of four common controlling authorities (ACC): Europol, Schengen, Customs and Eurojust.

## **5. *The group article 29 and the European Commissioner with the data protection***

### **5.1 The European Group of the authorities of protection**

Article 29 of the directive of October 24th, 1995 on the data protection and freedom of movement of those instituted an work group gathering the representatives of each independent authority of data protection national. This organization joining together the whole of the European CNIL has the role of contributing to the development of the European standards by adopting recommendations, to deliver opinions on the level of protection in third countries and advising the European commission on any project having an impact on the law and freedoms of the natural persons with regard to the data processing personal. G29 meets in Brussels in plenary session every approximately two months.

The CNIL is particularly invested in work of G29, the group of the European CNIL, which it chaired since February 2008. However, president Türk does not wish any more to chair this authority because of the obstacles related to competences of the members of this authority and his dependence relative to the various governments and institutions European.

### **5.2 The European Commissioner with the data protection**

The CEPD is an independent controlling authority from which the objective is to protect the data in personal matter and the private life and to promote the good

practices in the institutions and bodies of the EU. For this purpose, it fills the following tasks:

To control the data processing in personal matter carried out by the administration of the EU;

To give councils on the policies and the legislative texts which touch with the private life; and

To cooperate with the authorities of comparable nature in order to guarantee a data protection which is coherent.

## **Control**

The mission of control consists in checking that the institutions and bodies of the EU licitly treat the data in personal matter of the civils servant and other servants of the EU. The CEPD takes care of the respect of payment (EC) n° 45/2001 concerning the data protection which is founded on two essential principles:

1. The person in charge of the data processing must respect a certain number of obligations. For example, the data in personal matter can be treated only for given and legitimate purposes, which must be specified at the time of the data-gathering.
2. The person of which the data are treated - the person concerned - profits from a certain number of juridically protected rights. It is for example about the right to be informed treatment and right to correct the data.

## **Consultation**

The CEPD advises the European commission, the European Parliament and the Council for the proposals of new legislative texts and a whole series of other questions affecting the data protection. The mission of consultation primarily consists in analyzing the way in which the policies influential on the civil rights within the framework of the private life. This analysis contributes to a true debate of a political nature on the way in which one new legislative text can be effective while respecting as it should be freedoms of the citizens and by surrounding them of the desired guarantees. The councils allow the European legislators to better legislate by adopting laws in conformity with the European values.

## **Co-operation**

The CEPD cooperates with other authorities in charge of the data protection in order to promote a data protection which is coherent in all Europe. The laws as regards data protection are founded on common principles. In addition, for a

growing number of European databases, control is shared between various authorities (as it is the case for the Eurodac database). The central authority of co-operation with the national authorities of control is the Group of article 29.

The site of the CNIL is, today, a model of the genre.

The left-hand column gives access the essential headings:

Presentation of the CNIL - "Your rights" - "Your freedoms" - "your responsibilities" - "files" - "More".

The column of the medium differentiates two spaces: private individuals and professionals.

- 1) The private individuals can complain on line (with models about mails and "Your rights in question" and it ya a space "Young people".
- 2) The professionals are invited to declare (automated treatments of personal data), to reach their "draft of declaration" and the "Models of mentions CNIL", with a space dedicated to "All the declarations on cnil.fr".

For memory, a list of these principal fields:

**Bank-credit:** data protection applied to the financial questions; files of the banks, obligations of the professionals, credit, means of payment, taxation...

Consumption - publicity - spams: prospection with the development of consumer loyalty: the customers are targets but not victims! Discount cards, advertising Harassing, Junk emails... How to fight against the abuses?

**Territorial collectivities:** computerization of the services (civil statue, electoral rolls...), rise of controls (video watching, geolocalization...) : the local government agencies gain to play the chart of the protection of the personal data, that of the confidence of the citizens.

**Displacements - transport:** monitoring on the roads, reinforced controls in the airports, geolocalization: how to take into account the constraints of safety while respecting the freedom of going and coming anonymously?

**Numerical identity:** biometric titles of identity, navigations on Internet traced, rise of the inspecting devices of the people: thus is built the numerical identity, but vigilance is essential to preserve a private life!

**Internet-Telecommunications:** does the Internet threaten the private life? The data protection constitutes a response of topicality to the massive exploitation of the personal data of the Net surfers.

**Police-Safety-Justice:** the fight against the delinquency and terrorism intensifies: the files of police force multiply and grow rich by biometric data. STIC, Ed-

vige, Fnaeg, FIJAIS, Cassiopée, LOCATED...: to decipher these files and balance between safety and freedom.

**Health:** data of health: significant data subjected “the numerical” health proof: vital card, personal medical records, pharmaceutical file, Web doctor, electronic sheets of care...

**Information system security (ISS):** safety is conceived for the whole of the processes relating to the data, which it is about their creation, their use, their safeguard, their filing or their destruction. It relates to their confidentiality, their integrity, their authenticity and their availability

**Schooling - minors:** the protection of the young people is essential taking into consideration their daily use of new technologies. It is essential also that the monitoring of the children through biometric devices, the video watching or of the geolocalization respects their rights.

**Work:** new technologies work the work world: the field of human resources is largely concerned, while the monitoring of paid increases. The Data-processing law and Freedoms are invited in the debate paid employers/.

**Life citizen:** political communication, electoral roll, electronic administration, vote on line: is the life citizen put per hour of an easier daily life... but with which guarantees?

**Video watching:** generalization of the video watching in public space, with work, in the private buildings: this development must be accompanied by a better control of the respect by the rights and freedoms of the people.



# **The criminalization of hacking tools as a reasonable measure of protection regarding attacks against information systems and computer data**

---

---

**Konstantinos Chatziioannou**

---

---

## **1. New threats in the field of information security**

A number of programs, known as hacking tools, that could also be traced and downloaded via the internet, are used for the launching of attacks against information systems and electronic data. For example, we could mention programs that attack the confidentiality of computer systems, such as Trojan horses, but also programs, known as viruses and worms that threaten the integrity or availability of information systems and electronic data,

These programs could have enormous impact on the everyday life of individuals, provided they could attack the computer of every person, but also on the whole world, if these attacks are launched against the information systems of nuclear facilities. As a recent example, the worm “Stuxnet” could be mentioned, which has attacked a large number of industrial information systems of nuclear facilities in Iran by damaging their physical integrity, an event that heralds a new era of cyberwar (Menn/Watkins, 2010). Internationally there is a tendency of independent criminalization of the possession, production and distribution of hacking tools as a measure of fending off attacks against the confidentiality, integrity and availability (hereinafter c.i.a.) of information systems and electronic data. This paper is devoted to ascertain to what extent this is reasonable from the perspective of the protected legal interests.

## **2. International treaties that criminalize acts related to hacking tools**

According to Article 6 par. a) i) of the Convention on Cybercrime each contracting party is called to criminalize acts as the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily to commit committing any of the offences established under Article 2-5. In other words, the parties are also called to penalize preparatory acts of offences against the c.i.a. of computer data and systems. Let us stress, however, that this article shall not be interpreted as imposing criminal liability where the above acts are not for the purpose of committing

any of these offences, such as the authorized testing or protection of a computer system. Art. 6 par. 3 provides also provided that each party may reserve the right not to criminalise these acts, provided that the reservation does not concern the sale, distribution or otherwise making available of data by which the whole or any part of a computer system is capable of being accessed.

During the drafting of the Convention, articles', it was debated whether the devices should be restricted to those that are designed exclusively or specifically for committing offences. This perspective was considered to be too narrow, because it could lead to insurmountable difficulties in criminal proceedings, rendering the provision practically inapplicable (Explanatory Report of the Convention on Cybercrime, margin no 73). However, except for the submission of substantive to procedural criminal law, as it will be analyzed, this could cause many complications regarding the necessity of the general criminalization of hacking tools with a view to the protection of the c.i.a. of information systems and electronic data.

Is has been argued that the limitation of the Cybercrime Convention of criminalization by the requirement of an intent to commit specific crimes represents an adequate compromise (Sieber, 2004: 26). However, as this analysis will show, the criminalization of hacking tools could cause many problems.

On E.U. level, Framework decision 2005/222/JHA of the 24<sup>th</sup> of February 2005 on attacks against information systems did not criminalize the specific acts. The Proposal for a Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA that was submitted on 30 September 2010 by the Commission to the European Parliament and to the Council, prescribed in Art. 7 par. (a) the criminalization of the production, sale, procurement for use, import, possession, distribution or otherwise making available of any device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6, i.e. for committing offences against the c.i.a. of information systems and electronic data, without giving the opportunity to member states to express any kind of reservation. The lack of the possibility not to apply the provision under certain circumstances that is given for example in Art. 6 par. 3 of the Convention on Cybercrime has caused some considerations, and on 10 June 2011 the Council reached a general approach on the compromise text of the proposal. Art. 7 of the above Proposal for a Directive prescribes now that: 1. Member States shall take the necessary measures to ensure that the production, sale, procurement for use, import, distribution or otherwise making available of the following is punishable as a criminal offence when committed intentionally and without right, with the intent that it be used for the purpose of committing any of the offences referred to in Articles 3 to 6, at least for cases which are not minor:

- a) a computer program, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;
- b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.”. According to the above compromise text of the proposal the criminalization of other devices that are not programs and the criminalization of the mere possession of hacking tools are avoided.

Consequently, the following arguments that refer to the Convention on Cybercrime regard the specific Proposal for a Directive as well, which, in case of its adoption, will oblige member states, including Greece, to transpose such a criminalization to national law, without any possibility of limitation of criminal liability except for cases that will be considered as minor.

The present paper will focus on the criminalization of the production, possession and distribution of devices designed or adapted primarily for the purpose of committing any the offences against the c.i.a. of information systems and electronic data.

### **3. Considerations regarding the criminalization of preparatory acts against the c.i.a. of information systems and electronic data**

#### ***3.1. Problems that are related to the criminalization of all programs designed or adapted primarily for committing crimes against the c.i.a. of the information systems and electronic data***

As it is widely accepted in the civil law jurisdiction, a necessary prerequisite of criminalization is the protection of a legal interest (Kaiafa-Gbandi, 2000: 263 et seq. /Manoledakis, 1998/ Margaritis, 1981: 41 et seq. /Paraskevopoulos, 2008: 94 et seq. /Roxin, 2006: 8 et seq. /Simeonidou-Kastanidou, 2001, 25 et seq.). The protected legal interest of Art. 6 par. 1 a) i) of the Convention on Cybercrime could be considered the legal interests that could be endangered by the preparatory acts that are criminalized, i.e. the c.i.a. of information systems and electronic data that are endangered by acts that intend to commit illegal access, illegal interception, data interference and system interference.

It is argued that for the more effective combat of the dangers that are related to hacking tools (i.e. the creation of a black market for their production and distribution), the criminal law should prohibit specific potentially dangerous acts at their source, preceding the committing of offences against the c.i.a. of information systems and electronic data (Explanatory Report of the Convention on Cybercrime, margin no 71). So specifically, Art. 6 could be regarded as a provision

that protects the c.i.a. of information systems and electronic data at an earlier stage before the actual infringement of them. The main issue is if it is reasonable to protect the specific legal interest in such an early stage.

In the Explanatory Report of the Convention on Cybercrime it is mentioned that a similar approach has also been taken in the 1929 Geneva Convention on currency counterfeiting (Explanatory Report of the Convention on Cybercrime, margin no 71). However, it should be emphasized that Art. 3 par. 5 of the specific Convention provides that: "The following should be punishable as ordinary crimes: ....(5) The fraudulent making, receiving or obtaining of instruments or other articles peculiarly adapted for the counterfeiting or altering of currency". The main difference lies in that these tools must be peculiarly adapted for the counterfeiting or altering of currency and we could accept a form of distant endangerment of a protected legal interest. For the hacking tools, however, that are designed or adapted primarily for committing crimes against the c.i.a. of information systems it is not easy to trace from their nature if they contain a risk asset for the protected legal interest (cf. Kaiafa-Gbandi, 2007: 1086).

Besides, referring to computer programs that are used to committing crimes against currency we can refer to Article 149 of the German Criminal Code that penalizes whosoever prepares to counterfeit money or stamps by producing, procuring for himself or another, offering for sale, storing or giving to another 1... computer programs or similar equipment which by their nature are suitable for the commission of the offence. The criminalization of acts that are related to computer programs was introduced by a law that *inter alia* transposed the Framework Decision on increasing protection by criminal penalties and other sanctions against counterfeiting in connection with the introduction of the euro to national law (Law, 2002). Article 3 par. 1(d) of this document prescribes the obligation of criminalization of the fraudulent making, receiving, obtaining or possession of instruments, articles, computer programs and any other means peculiarly adapted for the counterfeiting or altering of currency. It must be emphasized that also article 4 of Framework Decision on combating fraud and counterfeiting of non-cash means of payment prescribes the criminalization of acts related to computer programs and any other means peculiarly adapted for committing counterfeiting or falsification of a payment instrument so that it will be used fraudulently.

While Article 149 of the German Criminal Code refers to programs which by their nature are suitable for these crimes, in German theory it is widely accepted that the suitability of the programs must be of a specific nature and only programs that are exclusively suitable for counterfeiting are penalized (Erb, 2005: margin no. 3/ Ruß, 2009: margin no. 3). In the relative Explanatory Report it is mentioned that in the devices that are criminalized a special applicability for

the execution of counterfeiting should be inherent by their nature (Stree/Sternberg-Lieben, 2006: margin no 3). In that case, the above programs are *per se* dangerous for the protected legal interest of currency and no specific problems of delimitation of the programs that are used for criminal purposes are created.

Furthermore, the German Federal Constitutional Court came to a strict construction of the purpose of software for the commission of such an offence against the confidentiality of electronic data that is prescribed in Art. 202c of the German Criminal Code, the provision that incorporated into national law the criminalization provided by Art. 6 par. 3 of the Convention on Cybercrime. The above provision of the German Criminal Law criminalizes acts that are related to software for the purpose of the commission of an offence against the confidentiality of data (Art. 202a and 202b of the German Criminal Code). This provision can be interpreted widely. Article 149 of the German Criminal Code was used by the German Federal Constitutional Court to demonstrate the equivalent interpretation that is formulated for the specific article that refers to devices that are suitable for the counterfeiting of money or stamps. More particularly, the court in the framework of a systematic interpretation mentioned specific provisions that refer expressly to the suitability of items for the committing of specific crimes (Articles 149 and 275 of the German Criminal Code). Under the Court Article 149 of the German Criminal Code in combination with its Explanatory Report is ordinarily interpreted so that in the measures of counterfeiting that are mentioned here is inherent a specific applicability for the committing of counterfeiting and this means that the specific measures should be suitable exclusively for the committing of counterfeiting (...). As a matter of fact, the Court came to the conclusion that we should perceive the term of purpose in Article 202c of the German Criminal Code more narrowly than the suitability or even specific suitability (BVerfG, 2009: margin no 62).

The above Court ruled that the programs that are subjective to the above Article 202c of the Germ. Crim.Code should be developed or adapted for the committing of specific criminal acts and that this purpose should have been manifested objectively (Id.: margin no 60). The mere suitability of the software for the committing of electronic crimes is not sufficient and programs which could merely be misused are not subject to the provision id. margin no 63) and we could not argue that the so-called dual-use hacking tools are included in Art. 202c of the German Criminal Code id. margin no 64).

Therefore, we should accept the criminalization of the programs that are exclusively adapted to the committing of crimes against the c.i.a. of information systems and electronic data. We should, however, mention that the letter of Art. 6 of the Convention on Cybercrime and of Art.7 of the Proposal for a Directive

on Attacks against Information Systems –contrary to the provisions of the above Framework Decisions related to the protection of currency and non cash means of payment- does not restrict the applying force of these provisions from widely interpreting the contents of the scope of this program. It entails programs that are designed or adapted primarily for the purpose of committing specific crimes and the applying services are in no manner restricted to covering the cases only that the exclusive scope of the program is the perpetration of a crime against the c.i.a. of information systems and electronic data. Furthermore the Explanatory Report of the Convention describes that the drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances (Explanatory Report of the Convention on Cybercrime, margin no 73). Consequently, the Explanatory Report of the Convention, contrary to the provision which was mentioned by the above Constitutional Court, could not easily support efforts to strictly interpret the term of purpose of the programs and devices respectively. All the more, they could easily support an interpretation that would include the specific programs to the *actus reus* of the crime and so would also penalize programs that are used in the field of security of information systems and electronic data.

Moreover, we should emphasize that the need of delimitation of hacking tools in comparison with the rest of the programs is even greater relative to the programs that are used to counterfeit currency. Programs that are suitable for the counterfeiting of currency are not at all useful for its protection. The authenticity of currency could for example be checked via special mechanisms. Contrary to that, tools that are designed or adapted primarily for committing crimes against the c.i.a. of information systems and electronic data constitute per se an essential part of the control of their security.

It should be emphasized that programs primarily adapted or designed for the purpose of committing crimes against information systems and electronic data are often used in the field of information security and in this way contribute to the further protection of their c.i.a. and not their breach. More particularly, these tools are usually used for the monitoring of security gaps and the development of security strategies (Stuckenberg, 2010: 43 et seq.). Consequently, an attempt to criminalize even the simple possession of such tools could pose innocent people in danger, while the proof of the further intent of committing a criminal offence against the c.i.a. of information systems and electronic data is very difficult in a digital environment.

The delimitation of the tools which are designed or adapted primarily for the committing of the above crimes is difficult. Programs are multidimensional and it is not easy to prove when there is an intent to breach the c.i.a. of information systems and electronic data. More precisely, this intent is always determined by people themselves and this in any case should be determined by objective criteria (cf. Cornelius, 2007: 685). However, the limits that are posed by them are indiscernible, provided experts in the framework of realistic examinations use programs that are designed for launching real attacks, for the simulation of attacks (Furnell, 2010: 181). Programs that are used by hackers are also used by companies in order to examine the passwords that are used by their employees (Borges, 2007: 8). Consequently, many hacking tools cannot be delimited from applications that are necessary for the security of information systems (Sommer, 2006: 68).

The internet also contributes to that development, by giving the opportunity to everyone and not only to information security experts to exchange those types of programs with the goal to deepen their knowledge in security issues. The criminalization of dual-use programs would deter the technological development and the improvement of the c.i.a. of information systems and electronic data, provided users would avoid possessing such types of programs due to their fear of possible criminal prosecution. This would result in the lack of control of the security of their information systems and electronic data and to the reduction of their protection in practice. As it has been noted, "the experimentation and joy to write a code a little more clever than the others and to infringe the others' countermeasures has always been part of the internet culture and many times hackers help us by torturing and perfecting our "immunity system"" (Papadimitriou, 2004: 30).

The ban of such tools would also create adversities to those who want to function legally and trace security gaps in information systems despite the reservation that is laid down in the Convention (Furnell, 2006: 290). Art. 6 par. 2 expressly provides that this article should not be interpreted as imposing criminal liability where the acts referred to in paragraph 1 are not for the purpose of committing an offence, such as for the authorized testing or protection of a computer system. However, this provision has a declarative character, and obviously in this case it would be difficult to determine exactly when these acts take place.

Regarding the allegation that criminalization is significantly restricted by requiring a further intent of committing a crime against the c.i.a. of information systems and data, generally in preparatory acts it is often difficult to determine the intent with clarity (Jescheck/Weigend, 1996: 523). Even more difficult is the attempt to delimitate the intent of committing a crime against the c.i.a. of information systems and electronic data in a digital environment.

### ***3.2. Problems related to the expansion of the power of the enforcement agencies***

By criminalizing the possession of a hacking tool without demanding the attempt of any offence against the c.i.a., law enforcement agencies are empowered to monitor all people that have a high level of technological expertise. Often, due to technical reasons it is difficult to prove a connection of an illegal access to an information system or electronic data and a particular program (Hilgendorf, 2009: margin no 5). This difficulty concerns all forms of attacks against the c.i.a. of information systems and electronic data because they take place mostly digitally. Generally, in the modern society, the concept of the “suspect” -to whom investigative measures could be imposed- has been enlarged and it is not always connected to the perpetration of a specific offence (Paraskevopoulos, 2009: 27 et seq.). Mere possession of hacking tools could refer to a large number of users of information systems. This could result in making suspects of individuals due to their electronic profiles, i.e. due to the mere habit of downloading software that could be used for criminal purposes. In other words, via the penalization of the possession of such programs, law enforcement agencies could monitor acts of possession without proving and reasoning the connection of specific tools to specific attacks against the c.i.a. of information systems and electronic data.

The determination of the purpose for committing a crime against the c.i.a of information systems and electronic data results to the unavoidable intrusion to fundamental rights of the users of information systems and data. And this stems the intent of such programs which could be examined mainly via the analysis and search of his information systems or the user's traces in the internet. However, these searches may often prerequisite some serious infringement of the protected legal interest of the c.i.a. of the information systems and electronic data of the possessor of a hacking tool, but also the breach of his fundamental rights, such as the confidentiality of communication, informational self-determination and private life (regarding the personal data of the user), but also the protection of the domestic sanctuary (when the systems are located in a protected area). They may also infringe the specification of the general right of personality (Art. 2 par. 1 in combination with Art. 1 par. 1 of the German Constitution) that covers the constitutional right for the warranty of confidentiality and integrity of information systems, as it was recognized by the Federal Constitutional Court (BVerfG, 2008: margin no 166) and could be based upon the Greek Constitution (Art. 2 par. 1 in combination with Art. 5 for the right of the free development of personality, but also Art. 5A regarding the information Society). It would be necessary to examine the information system of the possessor in order to determine if he had an intent to commit a crime against the c.i.a. of information systems and electronic



data. This kind of intent would rarely be expressed in accessible digital space, such as internet fora or elsewhere.

The intent of mere possession could not easily be proven. The above mentioned Constitutional Court of Germany, in order to clarify the controversial term of the purpose of the program, stated that what is needed apart from the purposes of the programmer, is an externally perceived manifestation of these scopes. This manifestation was related to the formulation of the program itself, by term of the use scope, which could be determined by the facts themselves (...), or by the sales policy and the advertisement of the manufacturer that clearly aims at illegal uses of the product (...) and the determination of the details is left to the competent authorities (BVerfG, 2009: margin no. 66). However, even if the above criteria could determine the purpose of people that produce or distribute hacking tools, they could not easily determine the purpose of the mere possessor that downloads a specific program.

Besides, the penalization of such acts is closely related to the possibility of search for means of evidence by the law enforcement agencies. In Nr. 8 of the Appendix to Recommendation No. R (95) 13 it is stated that criminal procedural law should be reviewed so as to make possible the interception of telecommunications and the collection of traffic data in the investigation of serious offences against the confidentiality, integrity and availability of telecommunication or computer systems (Council of Europe, 47). By already criminalizing the preparatory acts of offences against the c.i.a. of information systems and electronic data, we pave the way for the surveillance of the information systems of individuals and the investigative power of authorities is extended. On the other hand the protection of the legal interest of the c.i.a. of information systems and electronic data could be undermined, provided that the possible perpetrator of the possession of a hacking tool could be anyone.

### ***3.3. Additional problems regarding the criminalization of the mere possession of hacking tools***

The Explanatory Report of the Convention on Cybercrime provides that, as the commission of these offences often requires the possession of the means of access ("hacker tools") or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market for their production and distribution (Explanatory Report of the Convention on Cybercrime, margin no 71). Even if somebody accepted the existence of a black market, it is not at all certain that the consumer contributes to it, so that the penalization of the mere possession of the specific tools could be rationalized. Besides, the suppression of this phenomenon, for example in Greece, would marginally contribute to addressing the problem in third countries where these prod-

ucts could be produced. It is indeed sure that, given the international character of the electronic crime, there “safe havens”- countries could be set up where these acts are not criminalized, a possibility that is provided also for contracting states by the Convention in Art. 6 par. 3 referring to the formulation of reservation. For that reason, the fear that was developed in Germany during the transposition of the provision of the Convention that the criminalization of hacking tools endangers the financial existence of German information security companies and poses the tangible threat of these companies taking their operations abroad (*contra* Stuckenberg, 2010: 41).

The simple possessor of hacking tools contributes minimally to the creation of the specific market and this participation could not rationalize the penalization of his own act for the total aggregate that demands numerous actions (cf. Neumann, 2011: 206). The contribution of each possessor to the creation of the specific black market of production and distribution of hacking tools cannot rationalize the punishability of the mere possession, because in that case, we would impute a result (i.e. the demand through which the creation of a black market takes place) that occurs only by the collective demand for such tools. Besides, many times the so-called “black market” could also contribute to the implementation of greater safety by users, provided that the user of the information system uses such programs to monitor the safety of his system. We trace again the problem of delimitation of the term “black market” provided that the programs are not used exclusively for committing crimes against the c.i.a. of information systems and electronic data.

#### **4. Proposals regarding the criminalization of acts that are related to hacking tools.**

An obligation of Greece as a member state of the E.U. has not been fulfilled - via the final version of the Directive on attacks against information systems- for the criminalization of acts related to hacking tools. It was proposed during the ratification of the Convention on Cybercrime that was signed by Greece on 11/23/2001, to reserve the right that is prescribed in Art. 6 par. 3 not to criminalize acts related to the mere possession of hacking tools. In any case, the final version of the Directive should not oblige member states to criminalize the mere possession of hacking tools.

*De lege ferenda* for the other acts that are related to hacking tools the best solution would be to criminalize only the production and distribution of hacking tools according to Art. 6 of the Convention on Cybercrime that should be limited to tools that are exclusively designed or adapted to committing a crime against the c.i.a. of the information systems or electronic data. This way, we could avoid the

excessive expansion of punishability and would rationalize the criminalization of such preparatory acts that constitute a threat for the protected legal interest of the c.i.a. of the information systems and electronic data. A similar approach has already been taken for the delimitation of the term “weapon” in the Greek law (Kaiafa-Gbandi/Simeonidou-Kastanidou, 2008: 612 et seq.).

Programs are not so unrelated to the function of weapons as they may initially seem. There is also an opinion that information warfare has enabled states, as well as nonstate actors, to engage in armed conflict by way of bits and bytes instead of bullets and bombs (Brown, 2006: 190). Under this view, computer systems used to generate malicious codes may be classified as weapons, but other computer systems, telephone relay stations, satellites and other communications hardware that innocently and automatically transmit any signal they receive probably should not be classified as weapons (id., 185). Indeed, programs used in attacks against the c.i.a. of the information systems and electronic data play an equivalent role as weapons, but in that case, the direct target are the systems themselves and electronic data - not humans. We propose the adoption of the above criterion of weapon classification according to their exclusive use, to the hacking tools as well. Programs not exclusively designed or adapted for launching attacks against the c.i.a. are not *per se* dangerous to the protected legal interest and should not be criminalized.

Regarding the tendency to penalize acts that are related to the sale, distribution or otherwise making available of computer passwords, access codes, or similar data by which the whole or any part of a computer is capable of being accessed (Art. 6 par. 1 a) ii) of the Convention on Cybercrime and Art. 7 par. 1 b) of the Proposal for a Directive on attacks against information systems), it does not cause the above problems that have to do with hacking tools. These data are *per se* dangerous for the c.i.a. of information systems and electronic data and there are not many difficulties referring to the intent of the acts that are related to them. Mere possession of such data could remain, according to Art. 6 par. 3 of the Convention on Cybercrime, not punishable, and this is the reason why the user of the information system or electronic data could not easily be involved in a criminal proceeding. It would be more prudent, however, to provide the contracting states with the possibility to criminalize the acts of production and distribution of such data only in the cases that are related to a number of items, as prescribed in Art. 6 par. 1) b) for their mere possession.

## References

- Brown, D., (2006), A Proposal for an international Convention to regulate the use of information systems in armed conflict, 47 Harv. Int'L.J., 179-221.
- Borges, G. (2007), Advisory opinion on the Amendment on combating computer criminality [in German], 19.3.2007, 1-9.
- Cornelius, K. (2007), Referring to the criminal liability for the offering of hacking tools [in German], CR 2007, 682-688.
- Council of Europe, Committee of Ministers, European Committee in Crime Problems, Committee of Experts on Problem of Criminal Procedural Law connected with Information Technology (1995), Problems of criminal procedural law connected with information technology: recommendation No. R (95) 13 adopted by the Committee of Ministers of the Council of Europe on 11 September 1995, and explanatory memorandum
- Erb, V. (2005), in Münchener Kommentar zum Strafgesetzbuch, Verlag C.H. Beck München, § 149.
- Furnell, S. (2006), Cybercrime, Destroying the Information Society [in Greek], Papazisi Publications, Athens.
- Furnell, S. (2010), Hackers, viruses and malicious software, in Jewkes, Y./Yar, M. (ed.), Handbook of Internet Crime, Willan Publishing, 173- 193.
- Hilgendorf, E. (2009), in Leipziger Kommentar, 12th Edition, De Gruyter Recht-Berlin, § 202c.
- Jescheck, H.-H./Weigend, T. (1996), Textbook of Criminal Law [in German], 5<sup>th</sup> Edition, Duncker & Humblot, Berlin.
- Kaiafa-Gbandi, M. (2000), A look at millennium from the perspective of a member of the Greek criminal law community [in German], in Eser A./Hassemer W./Burkhardt B. (Ed.), German criminal law at the turn of the millennium: Review and outlook, München 2000, 261-282.
- Kaiafa-Gbandi, M. (2007), Criminal Law and Information Technology abuses [in Greek], Armenopoulos 2007, 1058-1087.
- Kaiafa-Gbandi, M./Simeonidou-Kastanidou, E. (2008), Jurisdictional applications of Special Criminal Laws [in Greek], Nomiki Bibliothiki..
- Manoledakis, I. (1998), The function of the concept of "legal interest" [in Greek], Sakkoulas Publications, Athens-Thessaloniki.

Margaritis, L. (1981), The legal object as a basis for the solution of interpretative problems of Article 224 of the Greek Criminal Code [in Greek], Thessaloniki.

Menn J./Watkins M. (2010), Warning over malicious computer worm, online at <http://www.ft.com/cms/s/0/e9d3a662-c740-11df-aeb1-00144feab49a.html>

Neumann, U. (2011), The criminal liability of the participant in the purchase, in Kaiafa-Gbandi, M./Prittwitz, C., Surveillance and criminal suppression (in Greek), Nomiki Bibliothiki, 199-210.

Paraskevopoulos, N. (2009), Targeting Majorities, New Orientations of Penal Control, in Serassis, T./Kania, H. /Albrecht, H.J. (eds.), Images of crime III, Representations of Crime and the Criminal, Duncker & Humblot Berlin, 27-43.

Paraskevopoulos, N. (2008), The foundations of Criminal law [in Greek], Sakkoulas Publications, Athens-Thessaloniki.

Papadimitriou, C. (2004), Life imprisonment to hackers? [in Greek], Kastaniotis.

Roxin, C. (2006), Criminal law, General Part, Volume I, The structure of the theory of crime [in German], 4th edition, Verlag C.H. Beck.

Ruß, W. (2009) in Strafgesetzbuch Leipziger Kommentar, 12th Edition, De Gruyter Recht-Berlin, § 149.

Sieber, U. (2004), Computer crimes, cyber-terrorism, child pornography and financial crimes, General Report for Round Table II of the 17<sup>th</sup> International Congress of Penal Law, in Spinellis, D. Computer crimes, Cyber-terrorism, child pornography and financial crimes, 11-50.

Simeonidou-Kastanidou, E. (2001), Crimes against life [in Greek], 2<sup>nd</sup> edition, Sakkoulas Publication.

Sommer, P. (2006), Criminalising hacking tools, Digital investigation, 68-72.

Stree/Sternberg-Lieben (2006), in Schönke/Schröder, Strafgesetzbuch-Kommentar § 149.

Stuckenberg, C.-F. (2010), Too much fuzz for nothing? (in German), wistra 2010, 41-46.

# **Private power and new media: the case of the corporate suppression of WikiLeaks and its implications for the exercise of fundamental rights on the Internet**

---

---

**Angela Daly**

---

---

## **1. Introduction**

In November 2010, the online non-profit media organisation WikiLeaks published classified documents detailing correspondence between the US State department and its diplomatic missions around the world, numbering around 250,000 cables. In order to maximise media exposure, five 'old media' publications (namely the newspapers Der Spiegel, El País, Le Monde, the Guardian and the New York Times) were given prior access to the material on the condition that they complied with common deadlines over when the material was released, with the result of this being that the correspondence was released in parts over the course of many days, dominating newspaper headlines worldwide. These diplomatic cables contained classified information comprising comments on world leaders, foreign states, and various international and domestic issues.

The reaction to WikiLeaks' release of these classified documents from the American political class was generally condemnatory of the decision to publish the information publicly, invoking national security concerns and the jeopardising of US interests abroad. There were also reports of the US Justice Department considering charging Julian Assange, the founder of WikiLeaks, with espionage offences based on the release of the cables.

In the wake of the political reaction, there was also a response from the corporate world, with various companies, such as Amazon, PayPal, Visa and Mastercard, ceasing to continue the provision of services to WikiLeaks.

In light of the above, this paper will firstly provide a detailed description of this corporate response to the Wikileaks controversy (section 2), prior to an assessment of the motivation for these actors to contribute to the suppression of WikiLeaks, to determine whether it is an example of Birnhack and Elkin-Koren's 'invisible hand' (section 3). The implications for freedom of expression on the Internet will then be analysed, especially in the situation of the infringer being a private actor constituting a mono- or oligopoly, before an examination of the legal resource open to WikiLeaks and its users for any infringement of fundamen-

tal rights (section 4). Lastly, the response to this corporate behaviour from the hacking community will be considered, particularly the Anonymous collective, to determine whether such exercises of corporate power on the Internet can be checked by employing technological means and whether hackers really are the defenders of online free expression (section 5).

## **2. The corporate response to WikiLeaks**

Various corporate entities with different links to WikiLeaks stopped providing services to the organisation subsequent to the release of the US Embassy cables. More precise details of these instances are provided below.

### **2.1 Amazon.com**

Amazon.com, the online company which started with selling books, has diversified into various other markets, including Amazon Web Services (AWS) which offers remote computing services over the Internet for other websites or client-based applications. WikiLeaks' website was being hosted by Amazon.com via these services prior to the US embassy cables controversy, yet on 1 December 2010 Amazon.com ceased to host the site. At first, Amazon.com did not comment on this cessation of service, but it subsequently issued a statement denying that either the government prompted them to stop hosting the site, or that mass-scale DDOS attacks prompted the website being taken off their servers. The company gave the reason for its actions as being that WikiLeaks violated AWS's terms of service, in particular the term stipulating that WikiLeaks must have all of the rights over the content posted online and that the use of this content must not cause injury to any person or entity. Amazon.com stated that it was 'clear' that WikiLeaks did not own or control all these rights over this content, and that it was 'not credible' that WikiLeaks could not have redacted the information in a way to ensure that 'innocent people' were not put in 'jeopardy'.

### **2.2 Apple**

The interaction between Apple and WikiLeaks consisted of an application being created for Apple's App Store, which was submitted to the App Store on 11 December 2010 and approved for sale on 17 December 2010 [Albanesius, 2010]. The App Store is an online shop where users of Apple hardware such as the iPad, iPhone and iPod Touch can browse and download applications for their device, some of which are free, some of which are available at a cost. The specific WikiLeaks App was created by Igor Barinov, a developer not associated with WikiLeaks, and was described as giving instant access to WikiLeaks' material. Furthermore, \$1 from every App purchased would be donated to WikiLeaks itself. On 20 December 2010, the App was removed from sale on the App

Store. According to Barinov's Twitter page, Apple gave no reason for its decision to cease offering the WikiLeaks App for sale.

### **2.3 Bank of America**

On 17 December 2010, Bank of America issued a statement saying that it would no longer process any transactions it believed to be destined for WikiLeaks, stating furthermore that its action was due to its belief that WikiLeaks may have been engaging in activities that were inconsistent with the Bank's internal policies for processing payments [Schwartz, 2010].

### **2.4 EveryDNS**

EveryDNS, a domain name system (DNS) management service provider which was WikiLeaks' hosting provider in the USA, dropped WikiLeaks from its entries on 2 December 2010, claiming in a statement that it had done so because the domain wikileaks.org had become the target of 'multiple distributed denial of service (DDOS) attacks, claiming that these attacks threatened the stability of EveryDNS's infrastructure, and thus threatening access to around 500,000 other websites.

### **2.5 MasterCard**

In early December 2010, the major payment processing company MasterCard announced that it would stop processing payments to WikiLeaks, with its reason for doing so being that WikiLeaks was engaging in illegal activity [McCullagh, 2010].

### **2.6 PayPal**

PayPal, a service which allows payments and transfers of money to be made via the Internet, announced in a statement dated 3 December 2010 that it would permanently restrict one of its accounts which was being used to raise funds for WikiLeaks, claiming that the account was violating its Acceptable Use Policy, since the account involved activities that 'encourage[d], promote[d], facilitate[d] or instruct[ed] others to engage in illegal activity'.

In February 2011, PayPal also suspended the account of Courage to Resist, an organisation raising money for the legal costs of Bradley Manning (a US army soldier arrested in May 2010 on suspicion of providing classified information to WikiLeaks – but not related to the US Embassy cables) [Indvik, 2011]. However, PayPal subsequently reversed its decision to suspend the account, claiming that the suspension had 'nothing to do with WikiLeaks', and instead the reason was



that Courage to Resist had not complied with PayPal's policy regarding non-profit organisations being required to link a bank account to their PayPal account.

## **2.7 Tableau Software**

Tableau Software, an American computer software company, provided data visualisation products to WikiLeaks for the contents of the leaked US embassy cables, subsequently removed them from the Internet on 1 December 2010. In a statement the company said that this was 'not an easy decision, nor one that we took lightly', but stated that the decision was based on their terms of service (in particular, users should not 'upload, post, email, transmit or otherwise make available any content that they do not have the right to make available') as well as the company receiving a request from Senator Joe Lieberman, the chairman of the Senate Homeland Security Committee, calling for organisations providing services to WikiLeaks to terminate their relationship with the website [Fink, 2010].

## **2.8 Visa**

Visa Inc., another major payment processing company, started suspending transactions destined for WikiLeaks on 7 December 2010 before carrying out an investigation into the organisation to determine whether its behaviour was contrary to Visa's operating rules. Visa Europe Ltd announced in January 2011 that it would continue to block donations to WikiLeaks until its own investigation was completed (which at the time of writing, has not yet happened).

## **3. A case of the 'invisible' handshake?**

This section will analyse the motivations for responses of the various corporations to the US embassy cables controversy, and determine whether it is an instance of Birnhack and Elkin-Koren's 'invisible handshake'. It will commence with an explanation of what this invisible handshake is, before continuing on to analyse these companies' behaviour in order to make this determination.

### **3.1 The 'invisible handshake'**

In their seminal article, Birnhack and Elkin-Koren (2003) identify what they call the 'invisible handshake' as the convergence of the interests of powerful private entities on the Internet and the State. The 'handshake' is 'invisible' since the average user/consumer/citizen is not usually aware of the extent of the cooperation between these two axes of power on the Internet, and this cooperation is often fairly clandestine and 'beyond the reach of judicial review'. Birnhack and Elkin-Koren posit that this interaction between government and its agencies, and mul-

tinational corporations produces 'the ultimate threat' to users' freedom on the Internet.

This state of affairs has come about due to the policies of the governments of various developed countries, particularly in North America and Europe, in adopting the role of regulator regarding the communications infrastructure, directing private behaviour through the use of rules, and thus in practice allowing the emergence of private entities in this environment, which exercise control over parts of the network. When the State wants to exert control over the network, it co-opts these pre-existing privately-managed nodes (2003). Birnhack and Elkin-Koren note that the State has become more active in the Internet from about 2000 onwards, due to 'its growing significance for commerce and community', and due also to geopolitical developments such as the use of the Internet by terrorists, especially in the wake of 9/11. The State is now functioning as an 'active player' on the Internet instead of a mere regulator, and is also acting using the Internet to fulfil its 'ancient duty of securing individual safety and national security'. To do this, the State co-opts private entities operating in the various layers of the Internet, either by obliging them to comply with State demands (through using legislative means) or by offering incentives for these entities to do so voluntarily. Although this is not abnormal behaviour from such States in their regulation form, until the 2000s such approaches had not been seen on the Internet, and the latter method of informally incentivising corporations to act in ways the governments want places such action firmly outside the scope of any administrative law checks, such as judicial review. One of the main reasons why these private entities are of interest to States is that by the nature of the products and services they offer, they simultaneously perform a monitoring function of the information that passes through their node of control, in particular being able to identify real-world, offline characteristics of the user.

Furthermore, Birnhack and Elkin-Koren (2011) argue that increased concentration in Internet markets and increased entry costs due in part to potential liability for users' behaviour (principally in the US) has limited competition between corporations on the Internet, and so limited options for users, and this is convenient for States since markets which are more concentrated are easier to govern. In addition, the potential liability of online service providers at least encourages and at most forces these Internet corporations also to exercise a policing function over their users, turning them into private enforcement agents.

### ***3.2 The motivation for cutting off WikiLeaks***

The companies considered above gave three types of reason for their decisions to suspend services to WikiLeaks: (suspected) violation by WikiLeaks of the company's terms of service; (danger of) damage to the company's technical infrastruc-

ture; and pressure from the US government, particularly in the form of Senator Joe Lieberman, to sever ties with WikiLeaks. Apple is the only company that gave no any reason for pulling the WikiLeaks app from its App Store.

EveryDNS was the only company which explicitly stated that it had terminated its relationship with WikiLeaks due to infrastructural reasons. In contrast, Amazon explicitly denied that this was a motivation for ending its relationship with WikiLeaks.

Tableau Software explicitly stated that part of its motivation to terminate its relationship with WikiLeaks was due to the request it received from Senator Lieberman requested it to do so. The decision to do so was strongly criticised by James Ball, who created the visualisation, claiming it 'smack[ed] of cowardice and blind censorship' [Arthur, 2010].

The other companies claimed that their motivation for ceasing to provide services to WikiLeaks was due to its behaviour (potentially) violating their internal policies, either because WikiLeaks did not have rights over the content, the publication of the content could endanger 'innocent people' (i.e. those persons whose names were mentioned in the leaked cables), or because WikiLeaks was more generally engaged in 'illegal' activity or encouraging others to engage in illegal activity (i.e. the actual leaking or dissemination of the leak of classified documents). However, these claims of illegality or lack of rights over the content are mere allegations since there has been no authoritative legal pronouncement on the matters, and the claims regarding the jeopardisation of the safety of individuals are also mere speculation. Furthermore, even if an illegal act was committed by the person who leaked the information to WikiLeaks, it would seem that WikiLeaks in disseminating that information enjoys the protection of the First Amendment vis-à-vis prosecution by the US Government [Benkler, 2011]. Nevertheless, the signals coming from Senator Lieberman were highly condemnatory of any corporate collaboration with WikiLeaks. Even though Amazon claimed its decision was wholly based on a potential violation of its terms of service, it had been in close contact with Senator Lieberman when coming to its decision. The Senator himself issued a statement saying that this was 'the right decision' and 'should set the standard for other companies'. Moreover, it is unclear what kind and amount of pressure was put on Amazon 'behind the scenes' by Senator Lieberman and his staff to sever its ties with WikiLeaks. Indeed, the Guardian claimed Amazon was put under 'heavy political pressure' to stop hosting WikiLeaks [MacAskill, 2010].

### 3.3 *The invisible handshake in cutting off services to WikiLeaks?*

None of the corporations examined were legally obliged to cut off services to WikiLeaks (e.g. none of them were served with a legal instrument specifically forcing them to do so). Despite that some of them explicitly stated that government pressure was not a reason for ceasing their relationship with WikiLeaks, there does appear to be in practice a manifestation of the invisible handshake between these corporations and the (US) government over WikiLeaks. The rhetoric of the US political class at the time was almost entirely against WikiLeaks' behaviour. The more sober rhetoric came from *inter alia* the White House. The White House announced that WikiLeaks had 'put at risk our diplomats, intelligence professionals, and people around the world who come to the United States for assistance in promoting democracy and open government', and termed WikiLeaks' behaviour 'reckless and dangerous action'. The US Secretary of State, Hillary Clinton, declared that WikiLeaks' disclosure of this information 'puts people's lives in danger, threatens our national security and undermines our efforts to work with other countries to solve shared problems [Jackson, 2010]. A more emotive statement came from Senator Mitch McConnell, US Senate Minority Leader, who called founder of WikiLeaks Julian Assange 'a high-tech terrorist' and said he should 'be prosecuted to the fullest extent of the law' [Curry, 2010]. Furthermore, there has been speculation about the possibility of a secret US grand jury espionage investigation into WikiLeaks [Beaumont, 2011].

Thus, there would appear to be at least a climate of moral and political if not yet legal condemnation of WikiLeaks' behaviour generated by the US government, and at most pressure and threats applied to the corporations facilitating the functioning of WikiLeaks. The corporations' response in cutting off these services to WikiLeaks would appear to fit into the conceptualisation of the invisible handshake as corporations being obliged or strongly encouraged by the government (with the possible threat of legal proceedings if the corporations do not comply with the government's demands). This way, by co-opting these private entities and their nodes of control, the US government has been able to make the functioning of WikiLeaks much more difficult (although not impossible, as despite the withdrawal of these services, WikiLeaks was still accessible on the Internet). This kind of behaviour from governments vis-à-vis corporations and vice versa is not unheard of. But instances of this happening on the Internet are growing in prominence, especially since in the 1990s such government/corporate control seemed unlikely. Indeed, this may be an attempt by governments of liberal democracies which place a strong emphasis on market mechanisms, such as the US, to manipulate the functioning of the Internet to approximate a new manifestation of Herman and Chomsky's 'propaganda model' of the mass media.

Indeed, Birnhack and Elkin-Koren (2011) themselves have commented on the case of WikiLeaks and the corporate response, and themselves identify it as 'a demonstration of an unholy alliance between government and large private corporations'. They note the 'shaky legal ground' on which the US government is standing when it comes to the legality of WikiLeaks' behaviour since, as mentioned above, even if the leak itself was illegal, its dissemination by a receiver of the leak such as WikiLeaks would seemingly be perfectly legal, and indeed protected from government interference by the free speech guarantees under the First Amendment to the US Constitution. However, attempts by private entities to cut off services to WikiLeaks are not subject to such Constitutional constraints protecting free expression and so constitute a more effective way of containing the leak.

#### **4. Implications for online free expression and legal recourse for WikiLeaks**

This section examines the implications of this government co-optation of corporations for free expression on the Internet, it looks in particular at what happens when the market in question is oligopolistic or dominated by one firm, such as the cases of the payment processing firms and Apple's App Store respectively. The legal recourse open to WikiLeaks and its users for any infringement of their fundamental rights will then be considered.

##### ***4.1 The implications of the corporate response to WikiLeaks for online expression***

The practical effect of these corporations cutting services to WikiLeaks is to stifle the freedom of expression of WikiLeaks itself, as well as the right of its users to receive this information. However, since these corporations are private entities, they are not subject in the same way as State agencies to the constraints contained in the First Amendment to the US Constitution or for that matter Article 10 of the European Convention on Human Rights (ECHR) protecting free expression in Europe. (The US and Europe were the primary arenas of the WikiLeaks controversy and the geographical locations of most of the actors involved, whether government, corporate, civil society or human individual – were either the US or Europe and so the jurisdictional focus of this piece). This issue extends beyond the scope of this particular incident involving WikiLeaks, and in fact highlights the extent of private entities' control over the Internet and the information disseminated over it. This gives cause for concern over civil liberties online: as MacKinnon (2010) puts it, '[w]hat is troubling and dangerous is that in the internet age, public discourse increasingly depends on digital spaces created, owned and operated by private companies'.

The relationship between Internet users (whether organisations such as WikiLeaks or individuals) and these Internet corporations offering products and services is governed by private arrangements (usually contract). In these private agreements (not with standing consumer protection law inserting certain terms into such contractual arrangements) the parties can stipulate the terms they wish and do not *prima facie* have to concern themselves with constitutional or treaty provisions on free expression. This is demonstrated in the corporations dealing with WikiLeaks giving as a reason for ceasing the provision of services as being WikiLeaks' (alleged) violation of their terms of service, to which WikiLeaks, when commencing using these services, agreed, and by which so was bound.

Yet, the logic of competitive markets for goods and services would suggest that even if the companies dealing with WikiLeaks cut off their services to the organisation, all is not lost: WikiLeaks merely needs to venture out again into the marketplace to obtain these services from competitors of these companies, which given WikiLeaks' demand for such services, ought to want to supply them.

However, if the market in question is not so competitive, either possessing an oligopoly or monopoly and if these corporations decide not to provide services to an organisation such as WikiLeaks, then WikiLeaks is in practice unable to procure these services from other sources and is effectively unable to disseminate the information it wants.

In the corporate responses above, the situation with the payment processing firms bears some resemblance to an oligopoly: the effect of Visa, Mastercard, PayPal and the Bank of America refusing to process payments for WikiLeaks dramatically reduced the possibility of donating to WikiLeaks. Indeed, it took mobile payment company Xipwire's positive action to facilitate payments to WikiLeaks for there to be a guarantee that those who wished could donate to the organisation (although this would appear to show that there are no, or low, entry barriers to this market) [Petrucci, 2010]. Thus, the power of such companies as Visa and Mastercard in the markets for payment processing, and in particular the level of control they can assert especially when combined, can be demonstrated by the fact that there have been various groups of legal proceedings against the two companies in both the US and the European Union for anticompetitive behaviour due to their large market shares. Furthermore, in light of these two companies cutting off services to WikiLeaks, members of the Dutch D66 political party in the European Parliament expressed fresh concerns over the companies' level of dominance in the European market, and in particular the implicit illegitimacy of the American influence over the blocking of payments from European citizens to a European organisation i.e. WikiLeaks [Dekker, 2010].

Moreover, there is the more monopolistic position of Apple over its App Store, which withdrew the WikiLeaks app in wake of the controversy over the US embassy cable leaks. For a user of Apple's iPad, iPhone and iPod Touch platforms, unless they 'jailbreak' the device, they can only run programmes approved by Apple and available via the App Store. 'Jailbreaking' one of these devices would be *prima facie* illegal in the US under the Digital Millennium Copyright Act as violating copyright law; however in July 2010, the US Copyright Office explicitly recognised an exception to the DCMA in this case, following a request from the Electronic Frontiers Foundation. Nevertheless, this at least gives Apple the power to control the Apps that are available to the users of its devices, and the ability to refuse Apps created by developers outside of Apple (such as the WikiLeaks App). There is the real potential for Apple to favour its Apps made in-house over Apps from external sources in an anticompetitive fashion, as well as exert some level of more ideological censorship over the kind of Apps that are available to the users of Apple devices.

Thus, the existence of a monopolistic or oligopolistic market worsens the circumstances for exercising the right to free expression on the Internet: in addition to the fact that constitutional/treaty guarantees of this right do not provide as weighty guarantees against infringements of the right by private entities as compared to governments, the existence of a mono-or oligopoly which acts in a way that impinges upon a user's free expression is even more detrimental since this denies or at least restricts even more the possibility of the user turning to a competitors to facilitate her free expression online.

#### ***4.2 The legal recourse available for corporate free speech violations***

Legal options open to WikiLeaks are considered below.

##### **Legal guarantees of free expression**

The right to free expression is protected in the jurisdictions under consideration by the First Amendment to the US Constitution and Article 10 of the ECHR.

##### **First Amendment to the US Constitution**

The First Amendment has traditionally been conceived of as a right enforceable against the American government, as opposed to a right enforceable against private parties such as corporations. Indeed, one way in which the American and European conceptions of free speech differ is that in the US not only is the First Amendment not enforceable against private entities such as corporations, but they themselves are considered to be 'speakers' and entitled to enjoy the right as well. The European approach centres more on the individual human person and is based on the ideas of autonomy and human dignity, and involves more govern-

ment regulation of expression, such as that emanating from legal as opposed to human persons, and hate speech.

Nevertheless, the limitations of this conception of the right to free expression in the Internet environment have been recognised. Yemini (2008) (writing in the context of the net neutrality debate but with conclusions on this issue which can be applied more widely) criticizes the 'traditional bilateral conception' of the First Amendment as the scenario of a conflict between a speaker and the (US) government and claims that this makes it inadequate for dealing with the 'multiple-speaker environment' found on the Internet. The issue with free expression and private entities in the net neutrality debate revolves around the fact that Internet Services Providers (which are usually private entities in liberal democracies) have the technological means to control and manipulate the information that Internet users send and receive. Yet they are not, under the traditional conception of free expression, subject to regulation on that basis, or indeed proceedings for infringement of the right. Yet, as explored above, the other layers of the Internet are similarly owned and controlled by private entities, which can exert their power in ways which are not in accordance with free expression.

Indeed, Benkler (2011) also recognises the difficulty in a First Amendment action in these circumstances. Certainly a direct action against the private providers under the current conception of the First Amendment is not possible, and it would be 'extremely difficult to bring action against the government or its officials' due to any pressure from the government that was applied to these private actors being indirect and subtle.

### **Article 10 of the ECHR**

The situation in Europe differs somewhat. Art 10 of the ECHR protecting free expression is an obligation primarily pertaining to contracting States, and is usually conceived of as a negative freedom. Nevertheless, the Article itself has been found to have some horizontal, positive effect in the case of *Khurshid Mustafa and Tarzibachi v Sweden* (2011, 52 EHRR 24) a dispute between tenants and their landlord over a satellite dish the tenants had installed to receive Arabic and Farsi language programmes against the terms of the tenancy agreement. In this case, the European Court of Human Rights (ECtHR) found that the applicants' freedom to receive information via satellite broadcast, which formed part of Art 10, had been violated as the State, Sweden, had 'failed in their positive obligation to protect that right'. It is possible that the reasoning in this decision could also be applied to the freedom to receive information on the Internet, and it could be argued that Internet users (as opposed to WikiLeaks itself) had this right infringed by companies such as Amazon refusing to host WikiLeaks. However, due to the WikiLeaks website itself migrating to different servers, as well as various 'mir-



ror sites' of WikiLeaks appearing in various other locations on the Internet, these attempts to 'shut down' WikiLeaks and prevent users accessing the information contained in the leaks did not work. The fact that users could still see this information would suggest that the Court would not find that their right to receive information had been violated. Nevertheless, again through the ECHR apparatus, the corporations themselves cannot be directly censured for their behaviour.

### **Alternative pathways for legal recourse**

Since the most direct legal protections of free expression cannot easily (if at all) be used against private entities, other pathways to upholding WikiLeaks' and its users' rights through the apparatus of private law will be explored below.

### **Competition law**

Given the semblance of a monopoly in the form of Apple and oligopoly in the form of the payment processing firms, this part will consider whether competition law ('antitrust' in the US) can provide any remedies which would in fact go some way to correcting the infringements of freedom of expression.

### **Apple**

In its position of control over the App Store, there is the possibility that Apple could be shown to be a dominant entity. It has complete control over the Apps which appear in its App Store even if they are created by other companies or individuals, and so could be said to be in a dominant position in the market for the provision of these services. However, since the practice of 'jailbreaking' Apple devices has been ruled to be legal in the US and is permitted in the EU, consumers can also choose to run apps from Apple's competitors' own app stores on their Apple devices. Nevertheless, if Apple is found to exhibit characteristics of a dominant position in the markets for apps (and particularly the market for apps for Apple devices), such as Apple's market share being enough for it to be considered dominant, then perhaps its refusal to allow the WikiLeaks app could be characterised as an abuse of this dominant position, in particular a refusal to deal or supply.

In the EU, a refusal to supply, while not explicitly listed in Art 102 TFEU (which prohibits abuse of a dominant position), has been recognised as an abusive practice in the case law. Firstly, it would have to be shown that Apple possesses a dominant position, which is defined in the *United Brands* (1978, ECR 207) case as containing two elements: an ability for the undertaking to prevent competition and to behave independently of its competitors, customers and consumers. Apple in its position of control over its App Store would appear to occupy such a position. However, the relevant market must also be defined over which Apple

is dominant – this could be the market for providing apps for Apple devices. Indeed, for Apple devices which have not been ‘jailbroken’ Apple is the only player in this market, whereas for Apple devices which have been jailbroken there are other app providers, so an analysis would have to be made of the extent to which Apple is dominant by e.g. looking at market share. Alternatively, the market for apps could be considered a sub-market, as in the *Kodak* case, in which consumers who have bought the main product e.g. an iPad are ‘locked in’ to the ‘sub-market’ i.e. apps from the App Store. Even if Apple is not dominant in the ‘primary’ market for devices, it could well be judged to be dominant in the sub-market.

Nevertheless, on the assumption that Apple is dominant in both markets or at least it is dominant in the (sub)market for Apps (which would seem *prima facie* to be the case), its decision to cease providing access to the WikiLeaks app could be characterised as an anticompetitive refusal to deal. Since the WikiLeaks app was initially available through the App Store, and was then suspended, Apple’s action in doing so would thus be the termination of an existing supply relationship, as established in the *Commercial Solvents* decision (as opposed to a refusal to supply a new customer, for which a distinction is made in the case law), resulting in the vertical foreclosure of the WikiLeaks app. Economic harm was suffered (since the WikiLeaks app was being sold through the App Store, with \$1 from each download being donated to the WikiLeaks organisation).

In terms of procedure, there could be public enforcement proceedings brought against Apple by the European Commission and/or the national competition authorities, in addition to private enforcement in domestic courts. If the former route is pursued, and Apple is found to have engaged in anticompetitive behaviour infringing Art 102, then large fines can be imposed on Apple by the Commission. Regarding the latter route, Art 102 has direct effect in the legal systems of Member States, and since the ECJ’s judgement in *Courage v Crehan*, there has been a right to damages for the breach of this Article in the legal systems of Member States. The WikiLeaks app may wish to seek injunctive relief in the form of an injunction to ensure access as an alternative to damages.

As regards the US position, the judiciary there has also developed the concept of refusal to supply, which in some cases constitutes an infringement of the Sherman Act. In light of the decision in *Verzion v Trinko*, it would appear that the American courts would follow a similar approach to their European counterparts in assessing the anti-competitive behaviour of Apple vis-à-vis the WikiLeaks app.

## **Payment processing firms**

The other potential source of a competition claim is the behaviour of the payment processing firms (Visa, Mastercard, PayPal and Bank of America) in refusing to provide services to WikiLeaks.

The most evident path to pursue here would be to show a collective dominance abuse by these firms, which in the EU is also contrary to Art 102. In order to show this, firstly the undertakings must together occupy a dominant position in the market, and here the market would be for payment processing (perhaps more specifically Internet-based payment processing). However, for an abuse of collective dominance to exist, there would have to be a 'link' between the firms i.e. some sort of agreement to behave in this way. This would have to be shown, although the 'agreement' could even be one of the payment firms telling the others that it was going to cease authorising payments to WikiLeaks. In the absence of such an agreement being able to be shown, some sort of oligopolistic interdependence between the firms could be argued, but the fact that another payment firm, Xipwire, managed to ensure that WikiLeaks could still receive payments would suggest that there were low entry barriers to this market, and so the argument of oligopolistic interdependence would not hold.

As regards US antitrust law, it would seem to be more difficult than in EU competition law to show an abuse of collective dominance, as this concept is less developed there as compared to Europe.

## **Contract and tort**

Given the nature of the agreements between WikiLeaks and the entities providing it with services, WikiLeaks may find it easier to obtain remedies in the traditional private law areas of contract and tort.

In the US context, Benkler (2011) recognises contractual actions as a possible route for WikiLeaks, based on a wrongful denial of service. He argues that the best path to take would be to argue that in the contracts WikiLeaks had with the commercial service providers, there was an implied contractual obligation not to withhold service unreasonably or without good faith, and that the obligation of good faith may be a sufficient basis for a court to examine the conduct of these service providers and sanction them for 'cutting off critical services to a client where that is done in order to suppress their speech'.

Benkler (2011) also considers the possibility of a US tort action, in particular the behaviour of these service providers being a tortious interference with the prospective economic advantage of WikiLeaks, but he acknowledges that it may be tenuous to demonstrate the economic advantage part of this for 'voluntary or-

ganizations' such as WikiLeaks. Nevertheless, this may be easier to demonstrate as regards the payment processing organisations since their ceasing of providing services to WikiLeaks was evidently aimed at preventing WikiLeaks from receiving donations which fund the organisation.

As regards the European picture, WikiLeaks would have to seek remedies in national courts (since contract and tort are still legal regimes mainly pertaining to the Member States' jurisdiction as opposed to coming under codifying, harmonising Europe-wide instruments). An interesting development in the contract law of some European countries (especially Germany, the Netherlands and the United Kingdom) is the process of 'constitutionalisation' of this area of law through the increasing application of fundamental rights to this regime. Thus, for example in proceedings for breach of contract between two private parties, it could be argued that the court should adjudicate the dispute in a way which protects fundamental rights. So in proceedings in such jurisdictions, WikiLeaks could argue that since its right to free expression has been infringed by these service providers breaching the contracts they had with WikiLeaks; and so a court adjudicating the breach ought to decide the case in a way which upholds WikiLeaks' right, taking the fundamental right to free expression into consideration when deciding whether the breach of contract was wholly unlawful or could be justified.

## **5. The postscript to the cables leak: hackers as the avenging angels of online expression?**

However, the saga of the corporate response to WikiLeaks did not stop at these corporate cessations of services. Indeed, there was yet a further extra-legal reaction, this time coming from the online hacking community. This section will analyse the hackers' conduct in particular the Anonymous collective, and determine whether corporate power infringing fundamental rights can be checked in this way, and whether hackers really are defenders of online free expression.

### ***5.1 Anonymous e-vengeance: hackers strike back***

In its own response to the corporate response to WikiLeaks in cutting off services, the Internet hacking community started to attack the websites of various of the corporate actors involved in this conduct, primarily under the 'Anonymous' umbrella. Anonymous is a decentralised, organised collective of hackers which acts in concert in an anonymous fashion, and over the last few years its focus has been actions promoting Internet freedom in general and freedom of expression online in particular. Anonymous's attention turned to the WikiLeaks controversy, and in particular the cessation of services from the payment firms under the moniker "Operation Avenge Assange", a substrand of Anonymous's broader "Operation Payback", which originally comprised distributed denial of service (DDoS) at-

tacks on opponents of piracy on the Internet, based on the fact they were infringing what Anonymous loosely considers as Internet freedom. In a statement on a website used by Anonymous, the collective claimed its extension of Operation Payback to attacking WikiLeaks' former service providers (particularly PayPal, which the statement explicitly mentions) was due to the censorious affront to online speech that these cessations of service represented [Correll, 2010].

After the announcement of the Operation Avenge Assange campaign, there was a number of DDoS attacks on the websites of the payment processing firms (and also EveryDNS, on 7 December 2010): Mastercard and Visa's websites were attacked on 8 December 2010, and on 9 and 10 December, two PayPal websites (thepaypalblog.com and api.paypal.com [port 443], respectively) were attacked, all being successfully brought down i.e. unavailable to Internet users for varying periods of time, which disrupted the companies' services as a result [Addley and Halliday, 2010]. There was also an unsuccessful attack on Amazon's website, which was aborted due to the fact it did not have an impact on the performance of Amazon's website due to its huge web-hosting capacity [Mutton, 2010].

## ***5.2 Hackers as David against the corporate Goliath in the fight for online free expression?***

Certainly, the actions of the decentralised yet coordinated hackers against the corporations which cut off services to WikiLeaks did manage to cause at least some disruption to the normal functioning of these entities, and gained a lot of publicity in doing so, compounding the negative media image of the companies. Indeed, Anonymous itself seems to have 'come of age', transitioning from 'cyber-pranksters' to full-blown 'hacktivists', using the same technical tools as industrial hackers for more explicitly political or ideological campaigns which are able to cause more damage to the systems of the targets [Cohen, 2010].

However, hacker groups such as Anonymous, especially given its seemingly horizontal control structure, are by their nature arbitrary: as regards free expression, it happens to be that they are affronted by the *de facto* restrictions on this right being exercised by WikiLeaks and its users, but they could easily shift their focus to another topic entirely, or act in a way themselves that infringes free expression, or other fundamental rights such as privacy. As regards the protection of free expression, or actions against infringers, hacker groups are not accountable or reliable in conducting these activities.

Furthermore, hackers themselves could be considered to be a type of "cyber-elite", or 21<sup>st</sup> century "digerati", since they have the technical power to conduct these kinds of cyber-attacks, and so require a certain amount of technical expertise, which may be beyond the skills of most normal Internet users. However,

in order to participate in these recent attacks coordinated via Anonymous, less technical knowledge seems to be necessary, so less technically-literate users can get involved – indeed, in some cases users merely needed to download a programme from one of the Anonymous websites and press ‘Run’ once they had done so in order to participate. Nevertheless, the less technically literate seem not to be so competent in covering their electronic tracks when participating in such initiatives (which would seemingly fall under the criminalisation of this conduct in various countries as constituting misuses of computing equipment), and there may yet be a distinction based on technical expertise inasmuch as the more sophisticated hackers are less likely to be apprehended by law enforcement agencies as they can ‘anonymise’ more effectively their online activity.

Nevertheless, the hackers’ response to the WikiLeaks saga shows that these Internet corporations are not entirely unstoppable behemoths in their conduct affecting free expression. While the legal regimes in place in the US and Europe may not provide wholly adequate remedies for free speech violations by private actors, the hackers’ activity shows that there are extra-legal, civil society-based means of expressing discontent at such infringements, and indeed ways of ‘punishing’ violators. However, the problems with this approach is the ‘mob justice’ nature of entities such as Anonymous, with their lack of accountability, legitimacy and reliability, and so they cannot be considered as sustainable and fair means of enforcing and protecting free expression on the Internet vis-à-vis corporations.

### **5.3 Conclusion**

So, where does all of this leave online free expression? The corporate response to WikiLeaks’ release of the US embassy cables highlights the fact that the current conceptions of free expression are inadequate for the Internet context, where expression depends on an increasingly privatised sphere. As has been seen with the counter-action from Anonymous, there has been a thankful coincidence that there is some reproach for the corporations’ behaviour from the hacking community. But, as detailed above, this is arbitrary, unreliable and capricious, as well as not preventing any similar future action in the same vein.

Pragmatically, entities such as WikiLeaks still retain the possibility of jurisdiction-shopping for the most favourable (virtual or physical) climate for online free expression e.g. by using servers based in such a jurisdiction, and engaging the services of companies also based there. For the continued and future enjoyment of free expression online, there is some hope on the horizon in the form of schemes such as Iceland’s Modern Media Initiative, which provides various legal guarantees and protections for freedom of information and expression online, and was in fact endorsed by WikiLeaks itself.

## Acknowledgements

The author would like to thank Benjamin Farrand and Giorgio Monti for their helpful and insightful comments on this piece.

## References

<http://loganleger.com/apple-app-store-antitrust>

Addley Esther & Halliday Josh, WikiLeaks supporters disrupt Visa and MasterCard sites in 'Operation Payback' Guardian 9 December 2010. Available at: <http://www.guardian.co.uk/world/2010/dec/08/wikileaks-visa-mastercard-operation-payback>

Albanesius Chloe, Apple Pulls WikiLeaks App from App Store PC Mag 21 December 2010. Available at: <http://www.pcmag.com/article2/0,2817,2374592,00.asp> <http://twitter.com/wikileaksapp>

Anonymous. Although due to the decentralised nature of Anonymous it is conceptually and practically difficult to define a single 'official' website. However, the two main websites for Anonymous or at least portals at the time of writing seem to be <http://anonops.net/> (and associated Twitter feed) and <http://hbgary.anonleaks.ch/>

Amazon, Web Services message. Available at: <http://aws.amazon.com/message/65348>

Ardiyok Sahin (2008), Comparative Analysis of Collective Dominance. Journal of Yeditepe University Faculty of Law, Vol. 3, No. 1, 2006. Available at SSRN: <http://ssrn.com/abstract=1162187>

Associated Press No proof WikiLeaks breaking law, inquiry finds Salon 26 January 2011. Available at: [http://www.salon.com/news/politics/war\\_room/2011/01/26/wikileaks\\_not\\_breaking\\_law/index.html](http://www.salon.com/news/politics/war_room/2011/01/26/wikileaks_not_breaking_law/index.html)

BBC News Cyber attack forces Wikileaks to change web address 3 December 2010. Available at: <http://www.bbc.co.uk/news/world-us-canada-11907641>

BBC News Wikileaks release of embassy cables reveals US concerns 28 November 2010. Available at: <http://www.bbc.co.uk/news/world-us-canada-11858895>

BBC News Wikileaks' Visa payments suspended 7 December 2010. Available at: <http://www.bbc.co.uk/news/business-11938320>

Beaumont Peter, WikiLeaks demands Google and Facebook unseal US subpoenas The Guardian 8 January 2011. Available at: <http://www.guardian.co.uk/media/2011/jan/08/wikileaks-calls-google-facebook-us-subpoenas>

Benkler Yochai, *A Free Irresponsible Press*, forthcoming Harvard Civil Rights-Civil Liberties Law Review 2011. Available at: [http://www.benkler.org/Benkler%20Wikileaks%20CRCL%20Working%20Paper%20Feb\\_8.pdf](http://www.benkler.org/Benkler%20Wikileaks%20CRCL%20Working%20Paper%20Feb_8.pdf)

Birnhack Michael and Elkin-Koren Niva, *WikiHunt and the (in)visible handshake* openDemocracy 20 February 2011. Available at: <http://www.opendemocracy.net/michael-birnhack-niva-elkin-koren/wikihunt-and-invisible-handshake>

Birnhack, Michael D. and Elkin-Koren, Niva, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*. Virginia Journal of Law & Technology, 2003. Available at SSRN: <http://ssrn.com/abstract=381020> or doi:10.2139/ssrn.381020

Charles, Arthur *WikiLeaks cables visualisation pulled after pressure from Joe Lieberman* The Guardian 3 December 2010. Available at: <http://www.guardian.co.uk/world/blog/2010/dec/03/wikileaks-tableau-visualisation-joe-lieberman>  
Amazon Severs Ties With WikiLeaks 1 December 2010, Website of Senator Joe Lieberman (CT). Available at: <http://lieberman.senate.gov/index.cfm/news-events/news/2010/12/amazon-severs-ties-with-wikileaks>

Cohen Noam, *Web Attackers Find a Cause in WikiLeaks* New York Times 9 December 2010. Available at: <http://www.nytimes.com/2010/12/10/world/10wiki.html>

Correll, *Operation:Payback broadens to "Operation Avenge Assange"* PandaLabs Blog 6 December 2010. Available at: <http://pandalabs.pandasecurity.com/operationpayback-broadens-to-operation-avenge-assange/>

Curry Tom, *McConnell optimistic on deals with Obama* MSNBC 5 December 2010. Available at: <http://www.msnbc.msn.com/id/40517039/ns/politics/40516927>

Dekker Vincent, *Zorgen over dominantie Visa en Mastercard in Europa* Trouw 9 December 2010. Available (in Dutch) at: <http://www.trouw.nl/tr/nl/4324/Nieuws/article/detail/1800653/2010/12/09/Zorgen-over-dominantie-Visa-en-Mastercard-in-Europa.dhtml>

Fink Elisa, *Why we removed the WikiLeaks visualizations* Tableau Software website 2 December 2010. Available at: <http://www.tableausoftware.com/about/blog/2010/12/why-we-removed-wikileaks-visualizations>

Herman Edward and Chomsky Noam, *Manufacturing Consent: The Political Economy of the Mass Media* (1988)

Icelandic Modern Media Initiative. Website in English available at: <http://immi.is/?l=en>



Indvik Lauren, PayPal Halts Donations to Defense Fund for WikiLeaks Source Bradley Manning Mashable 25 February 2011. Available at: <http://mashable.com/2011/02/24/paypal-bradley-manning/>

Jackson David, Obama aides condemn WikiLeaks; Obama orders review USA Today 29 November 2010. Available at: <http://content.usatoday.com/communities/theoval/post/2010/11/obamas-team-faces-sensitive-diplomacy-over-wikileaks/1>

MacAskill Ewen, WikiLeaks website pulled by Amazon after US political pressure The Guardian 2 December 2010. Available at: <http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon?INTCMP=SRCH>

MacKinnon Rebecca, WikiLeaks, Amazon and the new threat to internet speech CNN 2 December 2010. Available at: [http://articles.cnn.com/2010-12-02/opinion/mackinnon.wikileaks.amazon\\_1\\_wikileaks-founder-julian-assange-lieberman-youtube?\\_s=PM:OPINION](http://articles.cnn.com/2010-12-02/opinion/mackinnon.wikileaks.amazon_1_wikileaks-founder-julian-assange-lieberman-youtube?_s=PM:OPINION)

McCullagh Declan, MasterCard pulls plug on WikiLeaks payments Cnet News 6 December 2010. Available at: [http://news.cnet.com/8301-31921\\_3-20024776-281.html](http://news.cnet.com/8301-31921_3-20024776-281.html)

Mutton Paul, Operation Payback aborts attack against Amazon.com Netcraft 9 December 2010. Available at: <http://news.netcraft.com/archives/2010/12/09/operation-payback-aborts-attack-against-amazon-com.html>

PayPal Statement on Courage to Resist Situation PayPal blog 24 February 2011. Available at: <https://www.thepaypalblog.com/2011/02/paypal-statement-on-courage-to-resist-situation/>

PayPal Statement regarding WikiLeaks 3 December 2010. Available at: <https://www.thepaypalblog.com/2010/12/paypal-statement-regarding-wikileaks/>

Petrucci Joe, Philly mobile payment startup Xipwire collecting donations for WikiLeaks Flying Kite 7 December 2010. Available at: <http://www.flyingkite-media.com/features/xipwirewikileaks1207.aspx>

Schwartz Nelson D., Bank of America Suspends Payments to WikiLeaks New York Times 18 December 2010. Available at: [http://www.nytimes.com/2010/12/19/business/global/19bank.html?\\_r=1](http://www.nytimes.com/2010/12/19/business/global/19bank.html?_r=1)

Yemini Moaran, "Mandated Network Neutrality and the First Amendment: Lessons from Turner and a New Approach". Virginia Journal of Law and Technology, 2008. Available at SSRN: <http://ssrn.com/abstract=984271>

Zencovich Zeno, "La Liberta d'espressione Media, mercato, potere nella società dell'informazione" Il Mulino, Bologna 2004

# Rethinking about freedom and ethics in the era of networks: new trends in journalism ethics

---

---

Elsa Deliyanni

---

---

The evolution of digital technologies and the emergence of interactivity, as reflected in Web 2.0 applications, brought profound changes in the nature and organization of public communication. Many researchers refer to a 4th revolution, similar to the invention of typography<sup>1</sup>, with far reaching effects on media institutions, journalism, political communication, as well as cultural production, distribution and consumption<sup>2</sup>. In this context the evolution of freedoms, especially of those related to public communication of opinions and ideas, is inevitable.

According to liberal media theory, the role of Press and Media in modern democratic societies, is to facilitate democracy, by providing to citizens pluralistic information, helping them to shape their political opinion and to commit informed political choices<sup>3</sup>. Press and Media also operate as a Fourth Estate, or watch dog, aiming to seek and identify the truth, to control political power and report its deficiencies to society<sup>4</sup>. However, critical media studies approach, dealing with media power and democracy, has shown that the structure of the official mass media model, has gradually excluded citizens from public space and public deliberation<sup>5</sup>. The access into mass media communication has been limited to professional journalists, and political elites. This one way, massive distribution of messages has been adopted with the objective of creating and maintaining audiences for serving specific political and commercial reasons.

In opposition to the above model, the emergence of social media opened the gates of communication<sup>6</sup> to every citizen connected to the net. Strong research

---

1. J. McNamara, *The 21<sup>st</sup> century media revolution*, 2010, 2.

2. H. Jenkins, T. Dwyer, *Media Convergence. Issues in cultural and Media studies*, 2010, 5-18; *idem*, *convergence Culture – Where old and New media Collide*, 2008, 1-24.

3. J. McNamara (2010), 229-230; E. Deliyanni, *Media ethics*, Vol. 1 *Journalism ethics*, 2004, §85.

4. E. Deliyanni (2004), §§42-43.

5. E. Deliyanni (2004), §§45-46 and §51.

6. J. McNamara (2010), 221; Dan Gillmor, *We media*, Greek Edition, 2006, 85.

findings have shown the potential of this interactive converging media<sup>7</sup>, in reinforcing participation and solidarity, in enhancing of creativity and in constructing identity. At the same time, many pessimistic scenarios raise questions about the future of journalism as a profession and, moreover, about the quality and the accuracy of information distributed through the networks<sup>8</sup>.

The scope of this paper is to study the implications of Social Media and networks in the field of Journalism ethics. In the framework of Social Media key concepts and values, as objectivity, a concept strongly debated over the past decades, decline. However, as many scholars argue, the decline of objectivity<sup>9</sup> doesn't seem to lead to a "vacuum" of values in the field of journalism and New Media ethics. New Media are much more than deployment of communication technologies. As they all converge on the Internet they result in new communication practices, that are distinct from modern forms of mass communication as realized with Press, Radio, or TV<sup>10</sup>. These practices combined with the technological nature and structure of networks, along with the adoption of users' codes of ethics, create a new landscape in the field of social networks' ethics.

At first, we will present a brief history of the principle of objectivity. We will, then, study, how both journalistic practice and technology of Web 2.0. and networks are shaping ethics in this field.

## **I. Objectivity as a key concept in the field of modern journalism ethics**

1. *Journalism ethics' definition.* Journalism ethics and standards consist of ethical and good practice principles applicable to the specific challenges faced by journalists<sup>11</sup>. Generated directly from general principles of freedom of expression and functioning in a framework of Press self regulation<sup>12</sup>, they constitute guides to assist journalists in dealing with ethical dilemmas, when conflicts of interests are

---

7. H. Jenkins, The cultural logic of media convergence, *International Journal of Cultural Studies*, Volume 7(1): 33–43.

8. J. McNamara (2010), 229.

9. Ch. Atton, *Alternative journalism*, 2008, 84; Dan Gillmor, in *Reporters without borders, Bloggers' Handbook 2*, "What Ethics should bloggers have?" 2005, <<http://www.slideshare.net/Zash/bloggers-handbook2>>, *idem*, *The end of objectivity* [http://dangillmor.typepad.com/dan\\_gillmor\\_on\\_grassroots/2005/01/the\\_end\\_of\\_obje.html](http://dangillmor.typepad.com/dan_gillmor_on_grassroots/2005/01/the_end_of_obje.html)>, 2005.

10. J. McNamara (2010), 10; H. Jenkins (2008), 2-3, 254.

11. E. Deliyanni (2004), §§36-37; *Wikipedia*, <[http://en.wikipedia.org/wiki/Journalism\\_ethics\\_and\\_standards](http://en.wikipedia.org/wiki/Journalism_ethics_and_standards)>.

12. E. Deliyanni (2004), §36.

arise in the framework of journalistic practice. Principles of journalism ethics are usually incorporated in codes of ethics, which constitute statements drafted by professional journalism associations<sup>13</sup>.

2. *The appearance of the objectivity concept.* a) *Objectivity as a technical concept determining journalist's content.* The principle of objectivity is one of the fundamental journalists' professional ideals and constitutes the key ethical dimension of journalist practice. However its content has changed through time<sup>14</sup>.

In early days of Press, there was no reference made to objectivity. The commitment to truth constituted the fundamental principle and value of journalism. In U.S.A., this duty of the journalist to serve the truth was incorporated in the code of ethics adopted by the "Society of Professional Journalists". Journalists were bound to research, identify and report the truth<sup>15</sup>.

In a value centered media system, a system where journalists were serving democratic values and the public interest, the research for truth should necessarily lead to an accurate report of news. Even if incidents of lack of independence, truth and accuracy were not unusual, practices violating professional ethics' values could be seen more as malpractices of media proprietors. Thus, in the beginning of 20<sup>th</sup> century, journalists didn't separate facts from comments, and were regularly involved in political debates<sup>16</sup>.

The notion of objectivity as synonymous to universal truth has emerged in American Press during 20's and 30's and reflected the strict separation of facts from values. At that time, reality was impossible to be reliably constructed from state's points of views, due to the power of state propaganda campaigns. In this direction journalism had to invent a more rational method in order to permit citizens to form their opinion based on information close to reality. Journalism was trying at that time to establish itself on principles of sciences, as law and medicine. Expert and scientific journalism emerged and, alongside, impersonal fact centred practices and techniques of observation. In the framework of newspapers the facts and news had to be strictly separated from comments. Columnists were journalists whose work was to write strictly the facts. These journalists kept their freedom to write their comments in a separate place of the newspaper<sup>17</sup>.

---

13. E. Deliyanni (2004), §36.

14. Ch. Atton (2008), 84.

15. J. McNamara (2010), 230.

16. Ch. Atton, (2008), 84-85.

17. Ch. Atton, in Richard Keeble, *Communication Ethics Today*, 2006, 18-19, <http://www.google.com/books?hl=el&lr=&id=9LLnFThmdJEC&oi=fnd&pg=PA15&dq=alternati>

However, the adoption of the objectivity principle as an ethic value didn't fulfil the above expectations. In 1947, the Hutchins Commission on Freedom of Press in the US concluded that Press "wasn't meeting its responsibility to provide a truthful, comprehensive and intelligent account of the day's events in a context that gives them meaning"<sup>18</sup>.

Thus, one may assert, that the objectivity principle as "absolute universal truth", has never constituted a **general accepted value**. In the opposite, it has been continuously criticized by both journalism theory and practice.

b. *Ethical and political dimension of objectivity*. According to some researchers objectivity has risen not only as a technical issue, but as a moral claim as well. In this context, objectivity is something more than a claim about the kind of knowledge that may be considered reliable. It implies journalist's moral decision, concerning his position as an observer of the events taking place in the world, as well as the degree of his involvement. In this sense, objectivity constitutes a norm, or a guide and not a result that the journalist is bound to achieve, in relation to the content of his expression<sup>19</sup>. Moreover, objectivity is a political commitment "for it provides a guide to what groups one should acknowledge as relevant audience for judging one's own thoughts and acts"<sup>20</sup>. His duty is to report news "fairly and without prejudice"<sup>21</sup>.

c. *Objectivity in the field of alternative media*. Alternative Media aren't identified with New Media and blogging, since the former is not technology oriented and since this kind of Media existed from the early days of Press. The term Alternative Media, defines small scale media, which are more accessible<sup>22</sup> to the citizens than the mainstream ones.

In the field of alternative media (old and new) journalists, professional or not, have always taken under account the moral and political content of objectivity.

---

ve+journalism&ots=0KRD8WGe6d&sig=bPgrWe6W5pPEaM7mbIek6FYNIfs#v=onepage&q=alternative%20journalism&f=false>, 18.

18. J. McNamara (2010), 234.

19. Ch. Atton (2006), 18-19, <<http://www.google.com/books?hl=el&lr=&id=9LLnFThmdJEC&oi=fnd&pg=PA15&dq=alternative+journalism&ots=0KRD8WGe6d&sig=bPgrWe6W5pPEaM7mbIek6FYNIfs#v=onepage&q=alternative%20journalism&f=false>>.

20. M. Schudson, *Discovering the news: a social history of American newspapers, 1978*, 8; Ch. Atton (2008), 85.

21. <[http://en.wikipedia.org/wiki/Journalism\\_ethics\\_and\\_standards](http://en.wikipedia.org/wiki/Journalism_ethics_and_standards)>.

22. K. Coyer, T. Downumt, A. Fountain, *The alternative media handbook*, 2007, 1-5.

But, practitioners in this field have also questioned objectivity as well as impartiality from both an ethical and a political point of view<sup>23</sup>.

They always had little interest in “balanced reporting” and were very skeptical about impartiality. In the opposite, their expression was clearly biased and their selectivity proclaimed. Among scholars, Noam Chomsky demystified US mainstream media practices in relation to the objectivity principle, and provided the theoretical ground to practitioners, to do the same<sup>24</sup>.

The organization of alternative media is subject to the following ethical approach:

- Advertising is largely rejected, because external economic interests may affect the independence of their intellectual production. At the same time, advertisement is accepted for products and services approved by them: e.g. for similar publications belonging to communities with similar points of views.
- The concept of influence by the proprietor of the Medium is foreign to them. These media usually belong to non for profit organizations and have a participatory nature.
- They are community and public interest oriented and express loyalty and commitment towards their community. Very often, their loyalty is established and expanded at a transnational level<sup>25</sup>.

In respect to their practices, alternative journalists have elaborated a set of journalistic values ignored by scientific journalism and by scientific attempts at objective reporting.

## **II. Alternative journalism's practices shaping ethics in the field of social media and citizens' journalism**

*1. Introduction.* With the advent of Web 2.0 and social networks significant number of alternative movements was transferred to Internet, where they enlarged the field of their expression. There has been a massive explosion of alternative media during the last seven years (by means of blogs, web radios, WebTV, Twitter, etc.).

---

23. Ch. Atton (2008), 86.

24. Ch. Atton (2006), 18-19, <<http://www.google.com/books?hl=el&lr=&id=9LLnFThmdJEC&oi=fnd&pg=PA15&dq=alternative+journalism&ots=OKRD8WGe6d&sig=bPgrWe6W5pPEaM7mbIek6FYNIfs#v=onepage&q=alternative%20journalism&f=false>>.

25. See, for example, the Indymedia network model, in K. Coyer, T. Downumt, A. Fountain (2007), 70 and 78-79.

The emergence of blogs has shifted the concept of news from an authoritative objective or balanced account of issues and events, to a more subjective commentary that blends journalism with journal writing<sup>26</sup>. The practice of alternative journalists claims that a journalist cannot be objective, for that presupposes that an objective truth, an inviolable truth exists from an ontological point of view. Since objectivity is subject to the point of view of the observer, the absolute content of this concept fades away. Therefore, being objective is to present a story or a fact from different perspectives and points of view.

## *2. Alternative journalism's practices in the field of Social Media.*

i. Bloggers (citizen journalists) usually present their narratives, news and commentaries from the perspective of the individual (personal diaries by professional journalists or politicians, amateur investigative journalism, eye witness reporting by observers and participants)<sup>27</sup>. This kind of journalism focuses less on the journalist as professional expert<sup>28</sup>. Usually, the knowledge produced is the result of a close cooperation between the writer and the reader. It is a new way of thinking about journalism and a new way of producing journalism<sup>29</sup>.

ii. According to research findings regarding a group of bloggers formed by professional journalists and Iraqi citizen during the Second Gulf War, readers revealed that they trusted these bloggers because their method was "transparently subjective"<sup>30</sup> as they:

- didn't present their eyewitness reports as fact,
- didn't use their professional authority to shape readers' opinion
- didn't try to persuade readers that their version of events was reflecting the objective truth.

In this case, both writers and readers experienced the limits of objectivity, because readers' participation by means of questions, comments and proposals of leads, shaped bloggers' commentaries and eye witnessing.

This kind of practices represent the ideal in exercising journalism: they challenge objectivity and participation and confirm, at the same time the status of journal-

---

26. Ch. Atton (2008), 85.

27. Ch. Atton (2008), 83.

28. J. McNamara (2010), 226.

29. J. McNamara (2010), 250.

30. See detailed presentation of the study of D. Matheson and S. Allan, in Ch. Atton (2008), 94.

ist as an expert. Finally, ethical and political dimensions of the objectivity principle are recognized and taken under account<sup>31</sup>.

iii. Alternative journalism seeks also to invert the hierarchy<sup>32</sup> of access to the news, by explicitly foregrounding the viewpoints of ordinary people (of all those people whose visibility was usually obscured by mainstream media). Consequently, any story presented may use official as well as non official sources, which might be ignored by mainstream journalists.

This practice has a critical impact on the principle of representation, on the following grounds:

a) If the principal mission of journalists is to represent citizen by bringing his voice to the public sphere, then, by practicing the “inclusion”, journalists fulfil the above mission.

b) By allowing citizens to regain their access to media, the former are invited to participate actively to political processes. The inversion of access hierarchy to media achieved by means of this inclusion practice, leads to the establishment of a more democratic public communication model<sup>33</sup>.

iv. Alternative journalists use largely active witnessing (the subjects of the news stories are represented by themselves). This may be assessed as a threat to professional values, because a fundamental duty of a professional journalist is to refuse to participate as a subject in the news story he is reporting. But, does this way of reporting really threaten standards of objectivity to such an extent that it undermines trust in the profession of journalist?

Even in this case it has been argued that, this way of exercising journalism has a particular ethical dimension, since it contributes:

- In mobilizing public opinion, and
- In enhancing active participation and citizenship.

---

31. Ch. Atton (2008), 95.

32. Ch. Atton, *Alternative and Citizen Journalism*, in Karin Wahl-Jorgensen, Thomas Hanitzsch, “The handbook of Journalism studies, 2009”, 265-278, <<http://researchrepository.napier.ac.uk/2482/>>:

“To bring the voices of the local community into the centre of journalism is an ethical decision. This decision not only considers the local community as important (after all, the commercial local press makes the same claim), it also places these voices ‘from below’ at the top of the hierarchy of access, a practice that acknowledges ordinary people as experts in their own lives and experiences”.

33. Ch. Atton (2009), 265-278.



The most significant point in the field of alternative journalists' ethics is that differences and conflicts are freely expressed in the public sphere. Their subjective and partisan character is explicit and the purposes served are well exposed to the public<sup>34</sup>. Even if, due to their libertarian nature, they usually refuse to adopt their own codes of ethics, their practices reflect ethical choices which are clear and concrete; the public is, therefore, aware of them and free to adhere or not<sup>35</sup>.

Thus, we are moving from a modern precept "to report news objectively", founded on a universal perception of truth, to a post-modern subjective perception of truth<sup>36</sup>. This post modern subjective perception of truth predominates in the field of Social Media.

### III. Objectivity revised: the nature and structure of Web 2.0 as an open system, shaping citizen journalists' ethics.

1. *The loss of gate keepers, the withdrawal of journalism codes of ethics and the future of "objectivity" in Social Media and networks.* The advent of Social Media and the appearance of citizen journalists resulted in a publicly distributed information bypassing the traditional checking of content for compliance with legal norms and codes of ethics, usually undertaken by editors and legal departments in professional media organizations<sup>37</sup>. Alongside with the loss of traditional checking, filtering and balancing of sources, provided by mainstream media and professional journalists, we also experience a withdrawal of codes of journalists' ethics. In mainstream media these codes, functioning in the framework of media organizations or professional journalists' unions<sup>38</sup>, provided minimum guaranties for serving social responsibility values<sup>39</sup>.

Editors, journalists as well as a considerable part of media theory scholars, argue that this absence of gate-keepers in the new forms of media, result in a loss of truth, accuracy and credibility of information distributed on-line<sup>40</sup>. Inaccurate

---

34. See also T. Bolton, *News on the Net: A Critical Analysis of The Potential of Online Alternative Journalism to Challenge The Dominance of Mainstream News Media*, <[https://www.adelaide.edu.au/anzca2006/conf\\_proceedings/bolton\\_trish\\_news\\_on\\_the\\_net.pdf](https://www.adelaide.edu.au/anzca2006/conf_proceedings/bolton_trish_news_on_the_net.pdf)>, 9.

35. Ch. Atton (2008).

36. J. McNamara (2010), 231 and 250.

37. J. McNamara (2010), 221.

38. E. Deliyanni (2004), §67.

39. E. Deliyanni (2004), §49.

40. See, *Digital inspiration*, 5/6/07, *Bloggers vs Journalists – Pyjama army destroying Internet*, <<http://www.labnol.org/internet/favorites/bloggers-vs-journalists-pyjama-army-destroying-internet/278/>>, Regina INC, *Bloggers vs Journalists – Pyjama army destroying in-*

and misleading information is posted along with racial and sexist commentary; pornographic material abounds in on-line distribution of information. In these conditions, how is it possible to trust what's being said and written by citizen journalists<sup>41</sup>?

2. *Web 2.0 digital communities' self governance perception: systems' theory and the concept of "trust"*. In the early days of Internet, the majority of users –the so called netizens-, originating from the academic community, were mature citizens, capable for undertaking social responsibility and watching over the maintenance of order in cyberspace<sup>42</sup>. From these early communities of netizens comes the "cyber anarchist" perception according to which self-regulation in cyberspace may lead to censorship<sup>43</sup>. In the ideal public forum organized by citizen journalists, codes of ethics and disciplinary actions have no place and are impossible to function. Self regulation of blogosphere should result in a self-regulation of the entire society, which is rather utopian<sup>44</sup>.

At that moment, Tim Berners Lee (web's creator) deployed his efforts to turn this public space into an interactive one, where citizens could not only read, but also write and produce content. The fear that Internet might be controlled by States, governments and private economic interests, arose, then, as a serious danger.

Defenders of Internet's self governance established their arguments on general systems' theory<sup>45</sup>. Web 2.0 is considered as an open system because it exchanges information with its environment without limitations. A notion characterizing open and semi-open systems (like open societies) is the notion of trust, which is different from the notion of "assurance" evolving in closed systems (or societies). Open systems are capable of generating and developing relationships that exceed geographic and social boundaries, based on "trust". Trust is created and is attained in the framework of society through the proper management of honor and reputation of all its participants. The same is valid for digital communities, which are also open societies. The concept of trust among bloggers and their audience

---

ternet, <<http://regina-inc.com/?p=7547>; <http://www.newpartisan.com/home/pajama-pundits-mugger-takes-on-the-bloggers.html>>;

J. McNamara (2010), 222.

41. J. McNamara (2010), 223.

42. L. Mitrou, Self regulation in cyberspace, in, Th. Papahristou, Ch. Vernardakis, G. Theodossis, I. Kamsidou and others, "Self regulation", 2005, (in Greek), 75-78.

43. L. Mitrou (2005), 90.

44. L. Mitrou (2005), 88-91.

45. J. McNamara (2010), 7.

has a preventive and pedagogical nature<sup>46</sup>. Every member of the community is conscious that if he infringes ethical norms governing the community, nobody will trust him any more and his honour and reputation will be damaged.

3. *Social Media as a self-correcting entity*. Indeed, Social Media are demonstrating that they can act as a “self-correcting entity, where rigid regulation can be replaced by more flexible forms of organization”. Collective intelligence in knowledge communities incorporates a self-organizing form of editing and correcting of the user generated content. Web 2.0 offers important tools which serve transparency as<sup>47</sup>:

- The capability to post comments on blogs, wikis, and in social network sites as Facebook, You Tube etc. Thus, citizens are able to report errors and falsities.
- Devices permitting users to express popularity and trust also constitute paradigms where technology facilitates self regulation in the networks’ communities.
- Devices of linking give, finally, great accessibility to refer to sources of information (hypertext links). Users are, therefore, able not only to cite sources but also to control their accuracy. This characteristic reinforces the validity of research<sup>48</sup>.

In addition, we may notice that professional journalists are invited to play an important role in the field of Social Media, a new role which serves transparency and truth. Professional journalists are invited to counsel, advice, or provide guidance to users, to filter news, or to animate debates, using the tools, mechanisms and devices mentioned above. Certainly, they have lost most of their traditional privileges as they now, occupy an external position in relation to the content produced, but their participation in the whole process of communication is now more than essential<sup>49</sup>.

4. *Necessity and difficulties in adopting codes of ethics in the field of citizens’ journalism*. Since Read Write Web has become an over populated public space, where access is open and every anonymous user is free to produce news and influence public opinion, the debates concerning regulation of Social Media and networks

---

46. J. Ito, Weblogs and Emergent Democracy, <<http://joi.ito.com/static/emergentdemocracy.html>>, 2004.

47. T. O’Reilly, What is Web 2.0.: design patterns and business models for the next generation of software, 2005,  
<<http://oreilly.com/web2/archive/what-is-web-20.html>>.

48. T. O’Reilly (2005),  
<<http://oreilly.com/web2/archive/what-is-web-20.html>, 2>.

49. McNamara (2010), 225.

reappeared<sup>50</sup> and, occupy a significant place in the agendas, of various research fields, ranging from law to computers' science.

Some scholars have tested the limits of regulation by means of binding rules; others have proposed a mixed system of co-regulation. Yet, there is a unanimous agreement that the development of self regulation -by means of codes of ethics adopted by bloggers' and social networks' communities- is absolutely necessary.

Between 2003 and 2007 bloggers have been debating about ethic values<sup>51</sup> that Weblog community should follow. At that period, a differentiation has been made, between professional journalists' and citizens' blogs<sup>52</sup>. Non professional bloggers argued that as their Weblogs' form was more casual, they shouldn't be expected to follow the same ethics' codes as journalists<sup>53</sup>. However, it was soon made clear that even non professional bloggers should recognize they were diffusing news in the public space and that they had certain ethical obligations to their readers, the people they wrote about and society in general.<sup>54</sup>

Lasica tried to specify some general principles bloggers should follow. Between the basic values included in those proposals, we may notice the concepts of transparency, trust, honesty independence and integrity<sup>55</sup>.

---

50. J. D. Lasica, The cost of ethics: Influence peddling in the blogosphere <<http://www.ojr.org/ojr/stories/050217lasica/>, 2005>.

51. Dan Gillmor, in "Reporters without borders, Bloggers' Handbook 2, "What Ethics should bloggers have?", 2005 <<http://www.slideshare.net/Zash/bloggers-handbook2>>.

52. J.D. Lasica, The cost of ethics: Influence peddling in the blogosphere, 2005.

53. Dan Gillmor, A conversation about the future of journalism "by the people, for the people" <[http://dangillmor.typepad.com/dan\\_gillmor\\_on\\_grassroots/2005/03/the\\_gathering\\_s.html](http://dangillmor.typepad.com/dan_gillmor_on_grassroots/2005/03/the_gathering_s.html), 2005>.

54. R. Blood, the Weblog Handbook: Practical Advice on Creating and Maintaining Your Blog, Weblog Ethics, 2002, <[http://www.rebeccablood.net/handbook/excerpts/weblog\\_ethics.html](http://www.rebeccablood.net/handbook/excerpts/weblog_ethics.html)>; Cyberjournalist, A Bloggers' Code of Ethics <http://www.cyberjournalist.net/news/000215.php>, 2003>;

T. O'Reilly, Call for a Blogger's Code of Conduct, <<http://radar.oreilly.com/archives/2007/03/call-for-a-blog-1.html>>, 2007.

55. Disclose, disclose, disclose. Transparency – of actions, motives and financial considerations – is the golden rule of the blogosphere.

- Follow your passions. Blog about topics you care deeply about.

- Be honest. Write what you believe.

- Trust your readers to form their own judgments and conclusions.

- Reputation is the principal currency of cyberspace. Maintain your independence and integrity – lost trust is difficult to regain.

According to Gillmor, the fundamental purpose of bloggers' codes of ethics is to inspire to their readers trust and credibility. Objectivity is considered as an important quality but "impossible to achieve"<sup>56</sup>.

## Conclusions

The emergence of social networks and citizens' journalism introduces new practices in the field of journalism and produces new principles of ethics.

Thus, the changes in the field of journalism ethics can be resumed as follows:

- Key concepts of journalism ethics as the concept of "objectivity", decline.
- New concepts, as credibility and reliability, are requested to replace them.
- The concept of truth is shifted to the acceptance of distinct subjective perspectives of one and the same event.
- The above notions are specifications of a more general concept, inherent in Web 2.0 and digital communities, the concept of trust, from which they draw their conceptual legitimization.
- Technical structure and Web 2.0 tools, permitting self correction enhance self regulation through the maintenance of trust. At the same time, professional journalists continue to play their role of gate keeper. But their role is, therefore, external in relation to the content (since it is now produced by citizens).
- The state of co-regulation appears to constitute an appropriate response for regulating blogs diffusing information or blogs administered by professional journalists and may be imposed by law. This law should solely address the following issues:
  - to pose the operational framework,
  - to encourage and promote self regulation,
  - to define categories of blogs falling under its application field,
  - to impose the obligation of bloggers to post the ethical principles which are ruling the use of their blog. These codes of ethics should include principles of journalism ethics, adapted to the specific conditions prevailing in the blogosphere, and to the specific challenges faced by citizen journalists.

---

56. Dan Gillmor, in *Reporters without borders, Bloggers' Handbook 2*, "What Ethics should bloggers have? 2005, <<http://www.slideshare.net/Zash/bloggers-handbook2>>;  
*idem*, *The end of objectivity*, <[http://dangillmor.typepad.com/dan\\_gillmor\\_on\\_grassroots/2005/01/the\\_end\\_of\\_obje.html](http://dangillmor.typepad.com/dan_gillmor_on_grassroots/2005/01/the_end_of_obje.html)>, 2005.

- to introduce an independent supervision institution for blogs, by appointing a Weblog Ombudsman.

Finally, last but not least, digital literacy serves as a requirement for developing communication ethics in the networks.

# **IMEDIATV: Open and interactive access for live performances and installation art**

---

**Ioannis Deliyannis, Ioannis Karydis &  
Dimitra Karydi**

---

## **1. Introduction**

When the first television set was introduced to the public, it was advertised as a “Radio with a Screen”, implying that the listener would be able to simultaneously listen and view the musicians performing. Clearly, this was an understatement as the advanced capabilities, offered mainly by the optical stimulus, were overlooked at that time. Since then, television has been employed for many “novel” purposes, including the transmission of audio and visual content in the fields of recreation and education. Similarly today, interactive Internet broadcasting is often reduced to WebTV, as users are able to receive the same basic functionality over the web, ignoring all the new social, educational and experimental aspects that interactivity and virtual communication technologies have to offer (Tay and Turner 2009).

Various technological factors, marketing forces and content availability affect the deployment of these technologies. Established terrestrial and satellite broadcasting networks armed with strategic agreements with content providers traditionally attract the majority of viewers. In the technological forefront, one may contrast and analyse the battle in the 70’s between BETAMAX and VHS technologies in which the lower specification VHS standard was selected as it offered copying capabilities. Recent examples may also be referenced, one being the adoption of BLUE-RAY-DVD over HD-DVD where the availability of content won the battle of the formats. Therefore, content availability in the former may be identified as a principal factor that dictates which technological system will dominate the market.

During the last decade, users experienced rapid changes in the standards and formats of interactive broadcasting, a fact that may be responsible for the so-called “non-use non-adoption” phenomenon, that also affects the deployment of interactive internet-based TV (Webster 2004). Initial research conducted on autonomous interactive applications (Abascal and Civit 2001; Helena and Jorge 2001; Stephanidis and Akoumianakis 2001) was followed by the development of hybrid systems that multiplex various existing standards and formats in order

to successfully accomplish the task in hand across multiple software/hardware platforms and network configurations (Webster 2004; Martin 2005; Deliyannis 2010).

When the previously mentioned market trends are contrasted to the state of affairs today, where vast content is shared by users over freely accessible video posting and live event broadcasting websites such as YouTubeTV, one may safely assume that the TV of the future will not be a passive receiver and that it will most certainly involve a computerised application, enabling dynamic content selection from WebTV and other Internet broadcasting services. In fact, interactive television technologies that include dynamic video selection, computer-based content retrieval, and advanced interaction technologies such as passive or interactive movies and games (Silktricky 2010) have already been employed in various Information Society fields (Deliyannis, Antoniou et al. 2009; Deliyannis and Pandis 2009), furnishing or supporting entertainment, educational, commercial and research application domains (Jaimes and Sebe 2007).

Cost is another important issue that needs to be addressed. Typically, users are not willing to be charged for services that are already available from other providers either for free or at a minimal cost. The same condition applies when they are asked to replace their equipment with new devices in order to access new services. Characteristic is the case of the transition from analogue TV broadcasting to digital in Greece that involved a public campaign informing the viewers that they could utilise their existing viewing equipment, provided they purchase a digital decoder. Interactive broadcasting systems are affected, as charges on the use of propriety coders and decoders forces many to use open implementations that are freely distributable, or to develop their own. As a result, Internet-based interactive TV developers are forced to deploy open systems that support free player technologies in an attempt to attract a large user-base. In that respect, their supporting income is sourced from advertising and other means of promotion, which again is proportional to their user base.

On the positive side, decreasing Internet connection costs and increasing data transfer speeds allow the development of new interactive internet-based broadcasting services. With a dedicated internet-connection, one may receive at home high-quality TV programs, at a fraction of the cost of satellite TV. The authors believe that this is a quite significant development that allows new services to be introduced without the impracticality of replacing existing viewing equipment. Understanding user needs and broadcasting requirements is critical for successful adoption of the end-system by the users.

This article presents and discusses the experience gained in the development of an experimental low-cost interactive broadcasting station designed to present



specialised content in the field of interactive arts. Interactivity in that respect presents the end-user with several options that may either result into better content perception and understanding, or enable users to influence the presenter/performer and, as a result, the broadcasted content. The system presented in this work is designed to cover the needs for broadcasting quality, functionality, content accessibility, interaction and user-feedback, while, on the more experimental side, the overall aesthetics are addressed (Lovejoy 2004), as the art-based content requires particular presentation techniques to be employed. We conclude by discussing copyright issues that arise when content is spontaneously chosen and broadcasted live. Our work proposes the development of a licensing database enabling direct licensing of copyrighted content for direct utilisation in interactive broadcasting applications and performances, enhancing artistic expression and creativity.

## **2. User Requirements and Interaction Design**

The main purpose of our developing Internet-based interactive broadcasting station is to promote artistic student work designed and produced by students and faculty staff in the department of Audio and Visual Arts, Ionian University, Corfu, Greece. Under this scenario the station fulfils a principal strategic target of the institution as it permits student-artists to expose their work through a globally accessible medium without cost constraints. Content in the area of New Media Arts introduces complex presentation requirements, as it is media-rich and non-linear in certain instances. Therefore, when exposed to the public through interactive broadcasting features that include dynamic camera selection, voiceover and dynamic user feedback during live events offered through an open and expandable open source platform, content allows artists to comprehensively present their artwork in a dynamic manner (Deliyannis, Antoniou et al. 2009). The same infrastructure is used for the online and offline presentation of a wide variety of events organised by the department, such as talks, seminars, conferences, concerts, festivals and field trip recordings. System requirements are bound by various interaction design issues that are discussed below, describing how developers with network and cost constraints may utilise external services in order to cover particular user requirements while minimising the network and cost effects.

### ***2.1 From User Interaction Requirements to System Specification Design***

Content authors expressed certain presentation and interaction needs that had to be met by the broadcasting end-system. Video, audio and mixed-media artists requested that video and audio information should be presented as accurately as possible, with minimal loss in quality, in order to match the intended presenta-

tion requirements of the original content. This indicated to the development team that colour output and compression loss across a wide variety of signal coders/decoders should be evaluated and that an adaptive presentation system should be introduced, enabling the artist to set the broadcasting quality per clip. Initial analysis indicated that most of the submitted works are created or recorded in DV and DV-wide formats. Thus, although support for high definition (HD) information was not critical at this stage, the system should be able to support this standard, simply by altering the encoder at software level. Under the current system, this functionality is implemented dynamically as the intended broadcasting specification for each content item is stored in the content database within the stream metadata, enabling interested users to call on and view these streams on demand at their intended highest quality.

Interaction requirements were examined for various content types. First, the ability to access directly and choose the order of archived content playback is covered throughout with direct and dynamic linking to the archive. Metadata information may be added in two stages: the first set is added when the stream is uploaded to the server and includes entries that describe the streams' date, version, encoding and content format, total playing time, preview icon, stream-type and artist-information. At later stages, keywords and links may be added dynamically. The aforementioned metadata organisation enables the development of meta-searches according to user or program needs.

Three broadcasting modes are supported by the end-system: live events, video on demand and play-list broadcast of pre-recorded content. The same encoding method is employed for all three modes, while multicast broadcasting with a relay server is utilised in order to overcome bandwidth problems. Although the system employs the RTSP broadcasting protocol, enabling direct access from most networked devices via utilisation of the appropriate decoder, a web portal is provided in order to support the pre-recorded content broadcasting (<http://www.imediatv.eu/>), accessed via the VideoLAN player, an open source playback platform available under major operating systems. This organisation follows widely accepted standards, enabling, the reduction of the multimedia stream archiving cost that is a common problem for most low-budget broadcasting services. In order to reduce streaming and storage costs, support for external streaming storage and broadcasting is provided, through the utilisation of services, such as "YouTube" and "YouTube TV".

When comparing the proposed implementation with existing proprietary-broadcasting systems, one may notice various advantages. The first includes the availability of direct interaction with non-edited studio-sourced content, offering, for example, interactive camera selection to the user. This particular feature enables direct backstage access to the viewer, a feature that has already been used

to broadcast interactive multi-camera installation art content, permitting remote and non-edited exploration of the scene. Various events recorded with multiple cameras may be accessed independently, offering, for example, remote and interactive viewpoint selection. This may include stereoscopic broadcasts where left and right-eye information is transferred through separate channels. An additional feature is the availability of bidirectional live event broadcasting, enabling direct communication between the user and the studio performers or guests. This furnishes the broadcasting station with a plethora of live communication sources that may be employed beyond the typical viewer-presenter scenarios, for example, in the field of arts under telepresence scenarios, enabling remote user-artwork interaction. All interactivity options presented to the user are supported through the service's web-portal. RSS feeds and comment text forms provide user commenting and live dialogue, after registration and user verification, enabling text information to be communicated directly to the program producers and the participating members during live events. User feedback is also supported in video format, provided they are able to visually record and publish their response into the appropriate web-service linked to the stream. From the software-engineering perspective the spiral model was employed during system development. This allows the system to evolve and grow based on user and developer feedback, while it enables the addition of new functionality at later stages, as it is based on open source software.

## ***2.2 Development Through Open-source Code***

The above requirements do not pose significant developmental difficulties, as they utilise existing web technologies that require little or no programming and may be deployed in a wide variety of platforms (Spinellis and Szyperski 2004). Propriety or open-source code is provided for all the above uses, from the development of a complete "station portal" to the broadcasting method itself. The web interface is an essential aspect of the Internet based broadcasting system. The use of Content Management Systems (CMS) technologies such as "Joomla!" and "Drupal" allow the deployment of a fully customisable interface complete with RSS feeds, provide for the submission, editing and publication of online articles and supporting video-works stories, discussion areas with registered users and moderators, audiovisual galleries, as well as the existence of various administrative roles with variable access privileges and the ability to develop customised templates. The proposed system utilises a database-driven Joomla! installation, while the video database is held under PHPmotion, a free media-sharing CMS.

**Table 1.** Station requirements, standards and platforms supporting these technologies

Requirement	Protocol / Standard	Platform
Website	html, css, php, ajax	Windows, OSX, Linux
Archived Video Stream	unicast, multicast, H264	
Live Video Streams	Multicast H264	
Interactive Video Streams	multiple multicast servers, html, player	
Interactive User Feedback	html, rss	
Video User Feedback	H264, external service, html linking	

Most of the programming effort had to be focused on the design of the user interface with particular reference to its usability and aesthetics, as the open source technologies employed do not always share the same interface standards, a fact that requires end-system web-template modification. Developers have therefore to alter the look and feel of each individual component, resulting in a unified interactive environment, which covers the functional needs of both the user and the program producer. For the current case study in particular, the summarised technologies and platform choices can be seen in Table 1, where the developmental flexibility is clearly evident.

### 3. Content, Context and User Interface

Typical television stations base their functionality on time-based programming. The viewer is informed in advance by a timetable separated in program zones for each day about the order that each video stream will be displayed. For example, the daily news broadcast always begins and ends at specific times, usually presenting sports and weather reports towards the end. This is clearly an inefficient setting for Internet and satellite TV users, as they have to adjust their viewing experience according to international time. With interactive broadcasting the time-limitations are no longer present. The user is allowed to search and select the content to be viewed in live mode, or use a PVR-like function. Furthermore, as the individual components of the live broadcast may be produced in parallel, it should therefore be possible for a user who is only interested in the weather, to view the latest report on demand, or even watch the weather prediction for a specific area of the country. This major ability is mainly responsible for the differentiation between digital or WebTV to dynamic interactive TV, and the key requirement is hence to provide additional information regarding the information contained within the stream and its timing (Caschera, Ferri et al. 2007).

### 3.1 Content Retrieval

In this section a number of issues pertaining to multimedia content retrieval in an interactive internet-based TV station are discussed. It should be noted that some of these issues still remain open and, thus, call for further research.

**Importance and Requirements.** Identifying digital content desired from a pool of alternatives is an open research area as well as one of the cornerstones of the digital era. A number of difficulties make this research direction combining Information Retrieval and Data Mining challenging, such as the plethora of alternatives to consider, the timing requirements, the transient character of streaming volumes of alternatives as well as the interaction of users in the role of creators or contributors to the metadata of the data to be retrieved.

In the context of an interactive internet-based TV station, content retrieval is of great significance in order to assist user content selection, the importance of which was aforementioned, and avoid non-use and non-adoption. Nevertheless, such a process is not trivial, as a number of requirements need to be addressed: the intermingled persistent and transient character of content broadcasted, the augmented role of users/listeners in the Web 2.0 era and the need for integration of metadata, content-based and context retrieval for audio-visual data.

Interactive internet-based TV stations offer content that may be pre-recorded or can be a live event. To begin with, content retrieval in persistent databases (pre-recorded events) is not an easy process. Similarity definition can be based on any or all of (a) static textual metadata of the content, (b) content extracted features as well as (c) contextual information provided by users. To complicate matters more, streaming/transient data (live events) impose challenging requirements as memory limitations do not allow for buffering, data accumulation “on-the-fly” makes pre & post processing not a possibility, and high response time is a necessity.

**Persistent Data.** Persistent data information retrieval can be generally divided into categories based on the level/source of information operating. Textual metadata accompanying the data, such as title, date, and creator can be defined using a custom definition language. A number of frameworks attempt to standardise metadata with MPEG-7 being prominent in multimedia content description. Methods computing multimedia similarity using objective metadata, e.g., composer name, song title, etc. present an excellent methodology for content retrieval. The computing efficiency of textual retrieval based on the bounded definition language in combination with the unique source of objective information concerning the content make the use of metadata very important.

Still, in some cases metadata are of no use since these require prior knowledge of data that is not conveyed by listening/watching, may be unavailable (not set) and have limited scope due to usage of pre-defined descriptors. In these cases, content-based similarity has been under extensive research in a number of multimedia areas, focusing on features extracted directly from the datum content. These features express different attributes of the signal containing the datum that similarity can be based upon in order to retrieve content.

Despite the fact that content-based methodologies cater for query-by-sample, such methods base their distinction capability in the selection of descriptive features as well as the associated distance function. It is very common phenomenon that features and/or similarity function may not adhere to the characteristics required by users, thus diminishing the resulting efficiency of the retrieval process.

Contextual information is of great importance in similarity definition in all-human perspectives. Web 2.0 social services have offered unparalleled amounts of contextual information to “all things webbed” through the practice of assigning free textual labels (tagging). Bearing in mind the subjectivity of multimedia similarity and the nature of user assigned tags on data, it comes as no surprise that methods measuring multimedia similarity based on tags are in some cases reported more accurate than metadata or content-based methods (McFee, Barrington et al. 2010).

Rich as it may be in contextual characteristics, the information provided by Web 2.0 social services is known to present a number of disadvantages (Lamere 2008). Phenomena such as the “cold start” of new and not very popular data that have none or limited tags to work with, issues concerning synonymy, polysemy and noise of the assigned tags as well as tagger bias towards content preferred by young, affluent, and Internet savvy taggers affect enormously the effectiveness of this source of contextual information.

Accordingly, methods that integrate the previously mentioned methodologies of retrieval need to be devised in order to cope in an fully multimedia environment ,such as an interactive internet-based TV station since content retrieval is a key process. The integration of the methodologies will see that the effectiveness of the retrieval process will be ameliorated or at least retained in any case of user preference query or data form availability.

**Transient Data.** As far as the live events are concerned in this work, broadcasted data are confronted as streaming data/time-series received from a feed. Thus, data is modelled best not as persistent relations but rather as transient data streams. In that sense, broadcasted content shares a number of common characteristics with streaming data, such as being time ordered, data arriving in segments at

an unknown incoming rate and data storage/post-processing not being wanted/possible but instead an “on-the-fly” processing is required. Thus, methods utilised for similarity induction should be incremental in order to deal with memory limitations as well as high response time requirements. Moreover, streaming data methods are required in order to satisfy the need to use continuous querying, the scenario where a user receives data from a specific feed while a service monitors the remaining feeds in order to ensure that no other feed, is more similar to user requirements, in which case the user would be notified.

Furthermore, traditional information retrieval persistent relation models do not require a method for the identification of content semantic boundaries, as each section’s boundaries are clearly defined from a container file in the database used. Accordingly, if traditional retrieval methods are used in a data stream model, search for similarity cannot be stopped given that content/datum is early found not to be similar as no means of datum ending is provided therein.

Research in this direction is still very limited (Kontaki, Karydis et al. 2007; Ying, Beng et al. 2008). Nevertheless, the incorporation of such a capability in the proposed interactive internet-based TV station will be able to support the content selection in two of the fundamental levels of difference between the proposed station and WebTV, that is the provision of content search in live events as well as for more than one concurrent cameras (streams).

**The Role of Metadata.** The novelty of the current case study focuses mainly on the lack of content pre-programming. We focused on the essence of MPEG-7 in terms of content representation in our implementation, particularly as it was necessary to furnish the user with the flexibility to navigate semantically across the content. A typical example would include searching of semantically related works between different artists, in an attempt to artistically and emotionally describe with the use of video art selected notions such as “love” and “happiness” (Hansen 2004). One example that may be replicated under the current system is the categorisation of the works of a single artist in time, similarly to examples found on the WWW (Johnson, Shoopman et al. 2010). Under the current case study, another educational use may be the evaluation of the progress of a student-artist by viewing the published works in chronological order.

In order to achieve this functionality, descriptors are entered in a descriptor scheme (Caschera, Ferri et al. 2007), forming an informal yet dynamic Description Definition Language, as it is user-defined. Artists that upload a new video to the system are allowed to set the descriptors and the descriptor scheme of their choice. Other artists may choose to employ the schemes and descriptors already entered in the system, through drop-down menus, or create their own. In this respect we allow each creator to express their views and describe their content,

using their own customised expressions, which may not fall under an existing language vocabulary. There are instances, for example, that words, such as “woooooosh” and “ouch” are utilised to describe sounds within uploaded movies that alternatively would need to be described using many more descriptive words (Nack and Hardman 2002; Sivashanmugam, Verma et al. 2003). Once entered into the system, these are stored under the underlying XML description scheme. Note here that although we focus on accurate representation, the solution is to allow each creator to create their own vocabulary, a fact that allows semantic links to be made across the majority of terms. As this implementation is quite new, it is necessary to mature in order to evaluate its performance in the long term.

### ***3.2 User Expression in Web 2.0***

Web 2.0, following the analogy of software development numbering practice, refers to the evolution of Web 1.0. The key characteristic of the proclaimed evolution is the switch to interactivity in terms of interface, collaboration in terms of production and the centre-role placement of the website users in contrast to their previous passive character. Under the collaborative character previously mentioned, also lies a significant characteristic of the evolving web, which is the synchronous one-to-many and many-to-many communication capability of Web 2.0.

The amalgamation of Web 2.0 technology with the cultural domain affects all production, distribution, presentation, preservation and (re)utilisation of cultural expression. Cultural institutions are at a crossroad as to how to prepare for the new “wave of participation” that seems to be unavoidable. Reorientation of the institutions is necessary as the common practice of cultural activity through delivery of information reroutes towards an exchange between institutions and users.

Moreover, the roles involved are changing as well: all users, patrons, experts, customers, producers etc. involved in cultural activities are changed into participants, with their participating character stretching from consumption to interpretation or even contribution to institution artefacts. In addition to the obvious advantages that lead to this change, the enormous momentum of social networking services, the ease provided by e-services in contrast to their non-virtual counterparts as well as the epic scale of data included in their collections is putting additional pressure on institution for the adoption of similar practices.

In an attempt to categorise visitors of a museum, Mutanen (Mutanen 2006) came up with a generic classification for cultural institutions and their output audience. Accordingly, four categories of audience types are identified based on their relationship with the output of the institution as well as their participation - expression towards the output. Thus, the first category is titled “reactive consump-



tion” and refers to the simplest and most remote case towards any participation, in which the target audience of the output is solely consuming. Advancing a little the level of participation, “proactive consumption” implies that the audience has made some research on the output to experience and thus actively acquire information on the output. In the third case, “producing for private use”, the audience is materialising the experience of the output by means of talk, text, images or even video, though for a private use. In the final category, “producing for public use”, the proclaimed relationship includes purposeful sharing of the experience of the output the audience gained with others by reviewing, posting online or even tagging.

Nevertheless, many issues are get to be addressed (Middleton and Lee 2007) until the interactivity offered by Web 2.0 advances can be effectively put into practice by cultural organisations. Some of such key issues are (a) the media convergence based indistinctiveness of the institutions’ web 2.0 services when lending applications or characteristics from other institutions as well, which is based on studies of user preferences, (b) the capability to complement the authoritative information assigned by the creator/institutions on products by the collaborative wisdom of the web users, a.k.a. “crowd sourcing”, can alter the perspective of presented products for better or worse, (c) the potential of audiences to furnish information to objects presented in a web 2.0 service of a cultural institution proves to be quite an issue: e.g. what may have began as an image gallery can soon become a conversation under the auspices of the Web 2.0 service, and (d) the encouragement of user contribution to descriptions and perspectives of products requires new provisions to be made in order to ensure correctness of such an invaluable resource.

### ***3.3 User Interface Design***

When examining the organisation from top to bottom, one is introduced to the central menu of the interactive station. The web address registered (imediavt.eu) that displays the latest system version, clearly defines the objective of the service, while the logo is self-informative. The options offered at this stage are shown in Figure 1: “Interactive TV”, “News in Text”, “Program”, “Video Archive”, “User Settings”, “Submit your Content”, “BackOffice Access”, “Contact Us”.



**Fig. 1.** *Central menu choices of the internet-based interactive TV service, enabling information and interactive access to all features to the user over the web interface, through a unified web-based CSS animated menu.*

User interface design was based on the initial user requirements analysis which indicated that although interaction is the main program driver, a user transcending from traditional TV medium to Interactive TV would find this experience increasingly demanding, a major factor of non-use and non-adoption phenomenon. As a result, a principal design choice introduced is the provision of the default user with a pre-determined program, displayed under the "Program" option, that automatically displays the chronologically newest stream that is added to the system, while at every stage the user is presented with the option to select an alternative stream via keyword (content-context) selection. Upon selection of the "Interactive TV" option the player initiates and a supporting window is displayed, offering additional information about the stream displayed together with the related keywords.

#### **4. Enabling interactive content licensing for live broadcasts: practical and legal issues**

As already mentioned, broadcasting content within this web-based TV service covers pre-recorded material (on demand) and live events. Under the legal context, when it comes to making available pre-recorded material to the user which includes copyrighted works, the copyright holders' authorisation has to be obtained since such an act falls within their right to communicate the work to the public or to authorise the so doing under Greek Legislation (Articles 3(1)(h) & 1(2), Law 2121/1993). In the case of live event broadcasting, authorisation for the online communication of copyrighted works to the public, in our case

through an Internet-based TV service is also required (Article 3(1)(h) & 1(2), Law 2121/1993) (Stamatoudi 2009; Marinos 2004).

Having described the advanced functionality offered by the iMediaTV service where the live program content may be affected and altered interactively in a spontaneous manner, we propose the development of a digital networked database, enabling online and direct content licensing. In that respect, direct licensing of copyrighted works may act as a useful tool that benefits copyright holders, producers and users, while it permits freedom of expression to interactive new media artists. The presenter/ performer will be permitted to select material stemming from an open content pool, offering customised licensing services for multiple use scenarios. For example, a user may interactively provoke the presenter/ performer to create a derivative new media artwork based on the combination of existing ideas and works that need to be licensed before its creation. Accordingly, the database is used to link the presenter/performers' request to the copyright owners who have submitted the content to the database, and make sure that their licensing and cost conditions for the use scenario in question are met. The database functionality offers a series of services to the parties involved, which are described below.

Copyright holders are allowed to upload and register their content, use-conditions and royalties with the system. Completion of the registration process enables users to browse and select items from the database. When content is requested, then the system matches royalties with type of use, calculates charges where applicable and requests payment from the requesting user. After transaction is completed, content is delivered to the user, while the copyright owner is informed about the transaction. The user may alter the conditions and royalties declared at any point, and the system is updated instantly.

Direct licensing has already been introduced in the U.S. as a copyright licensing scheme for music, which creates a "one-to-one relationship" between the copyright holder and the end user of a copyrighted music track without the interference of any collecting society. Where the copyright holder is a member of a collecting society, there is still the possibility of engaging in direct licensing (*Buffalo Broadcasting Co v. ASCAP*, 744 F. 2d 917 2<sup>nd</sup> Circ. 1984). Such a license is granted for uses that are specifically defined, such as usage of the music track as background for commercials or its usage with other audio and/or visual elements, for instance, see [www.uniquetracks.com](http://www.uniquetracks.com) and [www.iamusic.com](http://www.iamusic.com). In other words, users will be allowed to "exploit" any of the works in the collective repertoire upon payment of a fixed fee without distinction as to the actual works used (Du Bois 1989).

Nevertheless, given the complexity of the implication of intellectual property rules on interactive media, some important issues such as the authors' moral rights or the monopolistic/dominate position that collecting societies have created within their territory should not be underestimated. Despite the fact that according to the Greek copyright law, it is at the author's discretion to assign the administration and/or protection of all or part of his economic rights to a collecting society (Article 54 (1), Law 2121/1993), the majority of authors prefer this scheme as they find it most effective for defending their interests. Besides, affiliation is often unavoidable with respect to those rights that by nature or statute cannot be administrated alternatively, for example under the specific cases where collective management is mandatory: (Articles 54(2), 57(8), 5(3), 18(3)-(11), 49(1)/(4)/(5), Law 2121/1993).

An interesting perspective that may offer an effective development for the proposed direct licensing scheme may come from the open content environment. It is only recently that a direct licensing platform, named "FAIRMUSIC", was established in Greece. Its available repertoire consists of musical works coming under the creative commons or content free of rights auspices and works of copyright holders who have not assigned any rights to a collecting society in Greece or abroad. Commercial licenses are obtained by paying fees for specific uses, namely "background music licenses" and "music licenses for multimedia projects", see [www.fairmusic.gr](http://www.fairmusic.gr). Despite this early attempt, collective management is still deemed a practically more viable choice (Marinos 2004).

The licensing database which we propose is an online per-work structured platform where copyright holders can directly submit their works, be it music or video, and define the specific uses allowed to the users, either for personal use or communication to the public (commercial) purposes including webcasting. Subsequently, users will be able to look for the work they are interested in, pay the relevant fees and lawfully obtain a relevant license of usage according to the pre-determined conditions. It may also include works under Creative Commons Licenses or even works free of rights (e.g. due to the expiry of the term of protection).

When communicating musical works to the public (as with broadcasting or webcasting), it is common practice to obtain blanket licenses from the relevant collecting societies, which cover a wide range of works in order to engage in the legitimate transmission of the specific copyrighted works that each society has been contractually assigned to administer (Marinos 2004). Nevertheless, therein lurks the risk of not using all the licensed material, while having already paid hefty royalties. Such a risk can be eliminated within the proposed licensing database scheme since the user will be able to identify the particular work interested in and get a license for the particular use of this work in a simple and quick way.

Accordingly, such a database will enable the broadcaster of the aforementioned Internet-based TV service to communicate to the user “right on the spot” any requested copyrighted content for which the former had not already obtained a license.

## 5. Conclusion

This work has presented a series of design, implementation, usability and legal issues that arise when developing an experimental web-based interactive TV service. An interactive broadcasting platform has been constructed, using existing individual components and technologies, open source systems and portals. From the computer science perspective, the system is designed to be customisable, platform independent and expandable, while a common XML-based database of content is used to synchronise and relate between the applications. New services may be easily implemented, enriching the end-system functionality.

Great interest lies in the methodology employed to interact with content, enabling the same system to simultaneously accommodate various interaction types: users may choose to watch the program without interaction, while at any stage they are able to link to other content of interest or influence live broadcasts via the bidirectional communication features supported. Content retrieval is discussed since it is a challenging and open issue, particularly for non-linear content with special presentation requirements. Moreover, the change of role of users due to the interactive features offered by the proposed service from consumers to participants is an open issue addressed by this work. Integrated media access, user participation, a uniform user-interface, dynamic content-access and open standards summarise the main factors that render such systems competitive and cost effective. Our paper concludes by proposing a direct licensing platform for interactive multimedia and interactive new media artwork.

## References

- Abascal, J. and A. Civit (2001). Universal access to mobile telephony as a way to enhance the autonomy of elderly people. Alc  cer do Sal, Portugal, ACM Press.
- Caschera, M. C., F. Ferri, et al. (2007). “Multimodal interaction systems; information and time features.” *Int. J. Web Grid Serv.* 3(1): 82-99.
- Deliyannis, I. (2010). Information society and the role of interactive multimedia, (in Greek).
- Deliyannis, I., A. Antoniou, et al. (2009). Design and Development of an Experimental Low-Cost Internet-Based Interactive TV Station. 4th Mediterranean Conference on Information Systems (MCIS). Athens.

Deliyannis, I. and P. Pandis (2009). An Interactive Multimedia Advertising System for Networked Mobile Devices. 4th Mediterranean Conference on Information Systems (MCIS), Athens.

Du Bois, R. (1989). Principles of Tariffs and distribution; some remarks on the most important activities of authors'rights societies. International Association of Entertainment Lawyers, Collective Societies in the Music Business.

Hansen, M. B. N. (2004). *New Philosophy for New Media*, MIT Press.

Helena, A. and F. Jorge (2001). The national initiative for people with special needs in the information society: the elderly, people with disabilities and long-term bed-ridden. Portugal, ACM Press.

Jaimes, A. and N. Sebe (2007). "Multimodal human-computer interaction: A survey." *Comput. Vis. Image Underst.* 108 (1-2): 116-134.

Johnson, J., D. Shoopman, et al. (2010). "YouTube Time Machine." from <http://yttm.tv/>.

Kontaki, M., I. Karydis, et al. (2007). Content-based Information Retrieval in Streaming Music. Pan-Hellenic Conference in Informatics.

Lamere, P. (2008). Social tagging and music information retrieval. *New Music Research* 37(2): 101-114.

Lovejoy, M. (2004). *Digital Currents: Art in the Electronic Age*, Routledge.

Marinos, Mihail-Theodoros D. (2004). Intellectual property (in Greek) A. Sakoulas, 2nd. edition.

Martin, B. (2005). "Information society revisited: from vision to reality." *J. Inf. Sci.* 31(1): 4-12.

McFee, B., L. Barrington, et al. (2010). Learning similarity from collaborative filters. International Society for Music Information Retrieval. Utrecht, Netherlands.

Middleton, M. R. and J. M. Lee (2007). Cultural institutions and Web 2.0. Fourth Seminar on Research Applications in Information and Library Studies (RAILS 4), RMIT University, Melbourne.

Mutanen, U. M. (2006). On museums and web 2.0 [Online]. from [http://ul-lamaaria.typepad.com/hobbyprincess/2006/06/museums\\_and\\_web.html](http://ul-lamaaria.typepad.com/hobbyprincess/2006/06/museums_and_web.html).

Nack, F. M. and H. L. Hardman (2002). "Denotative and connotative semantics in hypermedia: Proposal for a semiotic-aware architecture." CENTRUM VOOR WISKUNDE EN INFORMATICA (CWI)(INS-R0202).

Silktricky. (2010). "The Bank Run Game, The Outbreak, Crimeface." 2010, from <http://www.silktricky.com/>.

Sivashanmugam, K., K. Verma, et al. (2003). Adding semantics to web services standards. roceedings of the 1<sup>st</sup> International Conference on Web Services (ICWS'03).

Spinellis, D. and C. Szyperski (2004). "How Is Open Source Affecting Software Development?." IEEE Software.

The property right in Kotsiris L. & Stamatoudi I., Statute on Intellectual Property -Interpretation by article, Sakkoulas (in Greek).

Stephanidis, C. and D. Akoumianakis (2001). Universal design: towards universal access in the information society. Seattle, Washington, ACM Press.

Tay, J. and G. Turner (2009). "Not the Apocalypse: Television Futures in the Digital Age." International Journal of Digital Television: 31-50.

Webster, F. (2004). Universal Access in the Information Society, The Information Society Reader, Springer-Verlag, Routledge.

Ying, Y., C. O. Beng, et al. (2008). Continuous Content-Based Copy Detection over Streaming Videos. Proceedings of the 2008 IEEE 24th International Conference on Data Engineering, IEEE Computer Society: 853-862.

# Recent developments of the Bulgarian trademark legislation and practice

---

---

Jivko Draganov

---

---

## Introduction

The importance of the designations of origin in commercial activities has been out of the question for centuries. There is evidence for the use of signs capable of indicating the origin since the earliest data of commercial transactions<sup>1</sup>. Objectively nowadays a merchant can hardly act lawfully on the market without providing of certain minimum data regarding information of origin<sup>2</sup>. Protection of signs of origin under trademarks legislation reflects both the interest of the traders and those of the consumers. Moreover, it is also in close relation to the establishment of free competition rules on the markets. It is a small portion of companies that can afford to develop inventions, utility models, invest in new technologies, etc. or pay for licenses for their use, but every player on the market can enjoy trademark protection on relatively low cost. Therefore it is essential each market to rely on the appropriate legal framework that serves its development and corresponds to the interests both of the merchants and the consumers, and also providing guarantees that free competition will not be distorted.

The standards of trademark protection have passed a long way since the Paris Convention and the first national laws. They have been changing both domestically and internationally and on EU level providing a scope of broader protection of the trademark holders<sup>3</sup>. The establishment and functioning of the EU's Internal

- 
1. Brian Winterfield, Dow, Lohnes and Albertson, (March 2002), Historical trademarks, INTA Bulletin.
  2. Such as the ones established in the EU member states under the requirements of article 3, paragraph 1, (1) and (7) of directive 2000/13/ec of the european parliament and of the council of 20 March 2000 on the approximation of the laws of the Member States relating to the labelling, presentation and advertising of foodstuffs, Official Journal of the European Communities L 109/29.
  3. In the Decision of the Court of the EU *L'Oréal v. Bellure* (case C-487/07), in paragraph 58 the Court held that the function of the trademark "include not only the essential function of the trade mark, which is to guarantee to consumers the origin of the goods or services, but also its other functions, in particular that of guaranteeing the quality of the goods or services in question and those of communication, investment or advertising". See also Kur, Annette, Bently,



Market go through the adoption of secondary legislation in the area of trademark protection that influences national laws on one hand, and establishes a system for Community Trademarks Protection on the other. It has been more than 20 years now since the adoption of the first Directive<sup>4</sup> harmonizing the national laws in the member states, and almost the same time has passed after the adoption of the Regulation establishing the Community Trademark<sup>5</sup>. For that time the Court of EU and the national courts of the member states have ruled on numerous cases and still many questions are not less debatable. The Internal Market of EU needs appropriate, simple and clear rules for the benefit on the companies, the consumers and the market itself. These rules should be uniformly applied throughout all the territory of the Union. It would have been easier if the community trademarks (CTMs) were the only trademarks to enjoy protection within EU, but this is not the case and, even if we come to this point, it is still far in the future as it is not under question that both CTM and national systems will continue to coexist.

As national trademarks of member states enjoy protection there are many questions of significance both for the Member States and the Internal Market, which are answered by the relevant national laws and court practice. A company acting in two or more member states can find different legislative approaches to the registration and the protection of national trademarks<sup>6</sup> and different rulings by the national courts. As the Directive aims approximation of national laws limited only to those provisions which most directly affect the functioning of the Internal Market<sup>7</sup>, issues of major importance for the applicants and for the right holders, such as the procedures for registration or invalidity will remain subject matter of the relevant national laws. Nevertheless, the Directive does not establish rules for approximation in the areas mentioned above, so it seems that member states might find good reasons to follow the approach of the Regulation and adopt similar laws that would make the national procedures more attractive for the proprietors.

---

Lionel A. F. and Ohly, Ansgar, Sweet Smells and a Sour Taste - The ECJ's L'Oréal decision (August 17, 2009). Max Planck Institute for Intellectual Property, Competition & Tax Law Research Paper No. 09-12; University of Cambridge Faculty of Law Research Paper No. 10/01. Available at SSRN: <<http://ssrn.com/abstract=1492032>, accessed 29.03.2011>.

4. First Council Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks.
5. Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trade mark.
6. A comparison of the national trademark laws can be found in the OHIM "National Law Relating to the Community Trade Mark and the Community Design" compilation, <<http://oami.europa.eu/ows/rw/pages/CTM/legalReferences/nationalLaw.en.do>>, accessed 29.03.2011.
7. Recital (4) Directive 2008/95.

## 1. National trademarks legislation development in Bulgaria

Bulgaria, together with Romania joined the EU in 2007 and, thus, its market became part of the Internal Market of the EU. As a result of the accession, the CTM system spread its effect over the territory of the country, and since then the trends clearly show on increasing interest of the local merchants towards the CTM system<sup>8</sup> and a decreasing number of the national applications<sup>9</sup>. At the same time incomes from trademarks registrations is of major importance for the flow of the fees into the budget of the Bulgarian Patent Office<sup>10</sup>. There are several major factors influencing the choice of the applicants between the national and the CTM application, among which the awareness for the CTM system that is constantly increasing, the fees for the registration, that were recently lowered by OHIM, and the scope of the market activities of the local companies, that is enlarging due to the opportunities established under the free movement of goods and the freedom to provide services granted by the EU legislation. These negative trends for the national applications might be softened to certain extend by the latest amendments of the Law on Trademarks and Geographical Indications, introduced by the National Assembly<sup>11</sup> that entered into force in March 2011.

### 1.1 Change of the registration procedure

Since the Law on Trademarks and Geographical Indications which was adopted in 1999, the procedure for registration of national trademarks was based on ex officio examination for earlier rights. The latest amendments of Law introduce a switch form ex officio to an opposition procedure where the owners of earlier rights may invoke these rights in the process of registration. An opposition can be filed both for national and international applications by the holders of earlier national, CTM or international trademarks with effect on the territory of Bulgaria, as well as earlier applicants for such marks, by holders of well known trademarks and by licensees of exclusive licenses for such trademarks, by a pro-

---

8. The number of CTM applications from Bulgaria starts at 273 for the first year of EU membership and reaches 411 in 2010, OHIM Statistics by country, <[http://oami.europa.eu/country\\_reports/SSC003.1%20-%20Statistical%20travel%20pack%20by%20country%20%28BG%29.pdf](http://oami.europa.eu/country_reports/SSC003.1%20-%20Statistical%20travel%20pack%20by%20country%20%28BG%29.pdf)> accessed 29.03.2011.

9. The number of the national applications has decreased from 9170 in 2006 to 5140 in 2009 which is also 28% less than in 2008. See Bulgarian Patent Office, Annual Reports 2006, 2007, 2008, 2009, <[http://www1.bpo.bg/index.php?option=com\\_content&task=view&id=23&Itemid=150](http://www1.bpo.bg/index.php?option=com_content&task=view&id=23&Itemid=150)>, accessed 29.03.2011.

10. Just for one year (2009) the income from trademark fees has decreased up to more than 20%. BPO Annual Report 2009.

11. State Gazette N 80 from 12 of October 2010.

prietor of trademark against application by agent or representative, and at last by a proprietor of non-registered trademark, used in commerce on the territory of Bulgaria, for which an application was filed. The entitled parties are the same as in the Regulation, with one exception. The scope of licensees that can oppose is limited only to those with an exclusive license, while under the Regulation any licensee, authorized by the owner is entitled to act. Narrowing the scope of the entitled parties, licensees seem to have no objective grounds under the Law on Trademarks when authorized by the licensor, a licensee of non-exclusive license can undertake civil action at law before the court<sup>12</sup> and also have to be notified by the proprietor in case the latter intends to surrender the trademark registration<sup>13</sup>. It seems justified such a licensee to be recognized the right to oppose as it might be the interest of the proprietor, especially in case where the earlier rights are invoked on the bases of international or community trademark and there is no exclusive, but only non-exclusive licensee on the territory of Bulgaria.

The Bulgarian law deals in an unusual manner with the rights of the proprietors of earlier non-registered trademarks. The Directive<sup>14</sup> provides that member states can establish rules that grant certain rights to proprietors of earlier non-registered marks, namely to prevent from registration of these marks other parties and also invalidate such registrations. Under the Directive, as well as under the Regulation, the rights over non-registered trademarks are granted on the basis of earlier use of the trademark in the course of trade. Within the opposition proceedings the Law on Trademarks requires cumulatively use in the course of trade and application for registration for the non-registered trademark. Member states can decide if they will introduce protection of non-registered trademarks in their national laws, but once they do so the standards of the Directive have to be met.

The second condition of the Bulgarian law imposes to the proprietor to apply for registration of the earlier trademark in order to be entitled to oppose. But in case of applying for registration, the trademark will no longer be non-registered trademark, as after registration it will be protected since the date of the application as registered one. As a result the Bulgarian law actually does not provide protection of non-registered trademarks but rather grants some *sui generis* rights to applications of those who evidence prior actual use of the non-registered trademark in the course of trade. Signs used in the course of trade, even if not-registered, are

---

12. Law on Trademarks and Geographical Indications, Article 74.

13. Law on Trademarks and Geographical Indications, Article 24.

14. Directive 2008/95/EC, OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 October 2008 to approximate the laws of the Member States relating to trade marks (Codified version), Article 4, para. 4 (b).

protected against misleading use by other merchants under the Law on Unfair Competition.

### ***1.2 Opposition procedural rules***

The Law on Trademarks establishes a three months term for filing an opposition calculated from the date of publication of the application for national registrations. The notice for opposition should be in writing, in two originals, specify the grounds and include the arguments of the party. If needed the evidence may be submitted together with the notice of opposition. In case the earlier rights are invoked on the basis of well known mark or trademark with reputation, evidence should also be presented. It must be noted that the Law on Trademarks does not adopt the wording “trademarks with reputation”, as the Regulation and the Directive do in the official Bulgarian language version, but uses the descriptive “marks that are known”. In compliance to the requirements of the Directive, the Law on Trademarks includes among the grounds for refusal of registration earlier trademarks where the use of the later mark with no due cause would take unfair advantage or cause damage to the distinctive character or to the reputation of the trademark. Although it is clear that the so called “known marks” are actually trademarks with reputation, the use of different terminology for one and the same objects in the Law on the Trademarks, on one hand, and the Regulation and the Directive in their Bulgarian versions, on the other, may cause confusion and misinterpretation, especially where the mark with reputation is a Community trademark.

If the opposing party is not entitled to oppose or the notice is after expiry of the opposition period or no fee is paid, then the notice will be deemed inadmissible and no opposition proceedings will start. For other deficiencies, regarding opposing party details, the earlier trademarks or other rights, lack of arguments or evidence etc., the opposing party will be given two months to remedy them or otherwise the opposition proceeding will be terminated. Opposition procedure rules in general terms follow the ones of Commission Regulation (EC) No 2868/95. The examination is held by a panel of three experts. When opposition is found admissible, the notice and all evidence is communicated to the applicant of the opposed trademark. Both parties are notified and given three months to reach a settlement, whereas the latter period can be extended up to two more times under written request signed by both parties. If no settlement is reached, the applicant can rely on two months period to submit his observations, which are communicated to the opposing party. The opposing party then, in one month period will be expected to submit a statement. Under a request of the applicant, the opposing party should also submit proof of use of the earlier trademark during the period of five years prior the date of publication of the application of the opposed

trademark. Such a request can be made by the applicant not later than the expiry of the term for submission of first observations. Within six months after the end of the communication between the parties, the panel should issue its decision. The decision of the panel on the opposition is appealed at the Dispute Division, and the Dispute Division's decisions are subject to further appeal at the Sofia Administrative Court. More detailed rules regarding the examination procedure are expected to be adopted by an Ordinance issued by the Council of Ministers of the Republic of Bulgaria.

### ***1.3 Protection of well-known marks and marks with reputation***

Other important changes of the Law on Trademarks concern the determination of well known trademarks and trademarks with reputation. In 2006 provisions were included into the Law on Trademarks establishing special procedure at the Patent Office for determination of well known marks and marks with reputation that might be initiated on request of the proprietor after payment and furnishing of evidence. Under these rules a panel examines the request and based on its opinion, the President of the Patent Office issues a decision for determining if the trademark is well known or mark with reputation. The trademark, then, is being published and entered into the Register for five years period. The detailed rules were adopted in an Ordinance<sup>15</sup> that also governs in its article 2 (1) that "the status of a well known mark or mark with reputation on the territory of the Republic of Bulgaria is acquired after a decision of the President of the Patent Office based on statement of a panel appointed by him." The Law on Trademarks also provides that a well known mark or mark with reputation can be determined as such by the Sofia City Court in the course of civil proceedings, but the decision of the Court may not be opposed to third parties. After entry into force of the amendments of the Law on Trademarks in March 2011, no such procedure will be conducted, and well known marks and marks with reputation will be determined by the Sofia City Court or by The Patent Office within the opposition or invalidation proceedings. The abandonment of the "registration" of well known marks and marks with reputation is a result of the opposition system as no more ex officio examination for relative grounds will be held by the Patent Office.

---

15. Ordinance Establishing the Conditions and Procedures for Determination by the Patent Office of a Mark as Well-known mark and Mark with Reputation on the Territory of the Republic of Bulgaria, Promulgated in State Gazette N77 from 25 of September 2007.

### ***1.4 Absolute and relative grounds for refusal of registration and other changes***

While in opposition proceedings earlier rights may be invoked, the amendments provide any third party the opportunity to submit an observation against an application based on any of the absolute grounds for refusal of registration and, thus, the Law on Trademarks provides a mechanism for securing of public interest in trademark registrations. The wording of the rule follows Article 40 of the Regulation and these third parties will not be entitled to act further within the proceedings. The applicant is given the opportunity to submit observations and the Office will decide following the opposition procedure rules.

The amendments of the Law on Trademarks enlarge both absolute and relative grounds for refusal of registration. A new absolute ground for refusal refers to trademarks which include badges, emblems or escutcheons other than those covered by Article 6 of the Paris Convention and which are of particular public interest<sup>16</sup>. Such a trademark still might enjoy protection after receiving the consent of the proper authority. While the above rule clearly intends to serve the public interest, a new paragraph<sup>17</sup> of the Law on Trademarks might result in confusion. Before the changes, the relative grounds for refusal included the case where the applied trademark consisted of a geographical indication or derivatives thereof. Now the latter comes explicitly among the absolute grounds, but an exception is made when the applied trademark does not constitute of, but contains a geographical indication for which the applicant is entered as a registered user. The amended text provides that a trademark which contains geographical indication that is applied for registration or is registered on the territory of the Republic of Bulgaria or derivatives thereof shall be refused for registration unless the applicant is a registered user of the geographical indication. The Directive rest upon the member states to provide legislation where indications of origin constitute marks<sup>18</sup>, in particular allowing signs in trade that designate geographical origin to constitute collective, guarantee or certification marks. The Bulgarian Law on Trademarks establishes an exception that seems not to correspond strictly to the limitations set by the Directive. Problems might arise in relation of license rights granted of such trademark to third parties where no guarantees for certain characteristics of the goods in question will be assured by the licensee, as such might be established as for designating the goods of all registered users of the appella-

---

16. Council Regulation (EC) No 207/2009 of 26 February 2009 on the Community trade mark, Article 7, 1 (i).

17. Law on Trademarks and Geographical Indications, Article 11 (1) 13.

18. Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trade marks, Article 15 (2).

tion of origin that has been included into the trademark. Such situation might be prevented in a case where the trademark that contains the geographical indication can be only registered as collective or certificate mark. There is a provision under article 25 of the Law on Trademarks establishing that when use of the mark by the proprietor or by another person authorized by him is made in a way that users are misled as to the quality or geographical origin of the goods or services anyone is entitled to request revocation of the registration. Nevertheless limiting such registrations to only collective or certificate marks would provide more guarantees for avoiding the risk for the consumers to be misled by the use of the geographical indications.

Other amendments regarding relative grounds for refusal of registration define the meaning of “earlier trademarks” which corresponds to the wording of the Directive and the Regulation. New articles are added in order to prevent registration of a trademark by an agent or representative without the consent of the proprietor as well as registration of non-registered trademark that has been actually used in the course of trade before the application.

Finally, the amendments introduce changes into the terms for payments of fees that are shortened from three months to one month providing the option for payment after expiry of the term the double amount of the fee. It is a long expected step that was undertaken with the new rules to provide for on-line application for registration. After the changes, the Law on Trademarks finally adopts the on-line register of trademarks and on-line applications which will be a major ease for the proprietors and for the public to benefit more by the system for national protection of the trademarks in Bulgaria.

## **2. Parallel imports from the perspective of the Bulgarian court practice**

The exhaustion of the trademark rights has been one of the most controversial and debated issues after the establishment of the CTM system and even since the Treaty of Rome<sup>19</sup>. The Court of EU has ruled a number of times on this problem but is still being brought before national jurisdictions. That could easily be explained as the EU common market is a major target for parallel importers because it is an area with no internal boundaries where prices of original products are usually higher compared to many third countries' markets.

---

19. Calboli, Irene (2002), Trademark Exhaustion in the European Union: Community-Wide or International? *The Saga Continues*. *Marquette Intellectual Property Law Review*, Vol. 6, pp. 47-90. Available at SSRN: <<http://ssrn.com/abstract=802226>>, accessed on 22 March 2011.

## ***2.1 The Supreme Court of Cassation Interpretative Decision on Parallel Imports***

Bulgaria is no exception as the national courts have not been consistent in their rulings on parallel imports. During the early years of Bulgaria's EU membership many controversies in the judgments needed to be overcome. In 2008 the Chairman of the Supreme Court of Cassation requested the General Meeting of the Commercial Judges in order to interpret on certain articles of the Law on the Trademarks<sup>20</sup>. The request was made on the grounds of article 125 of the Law on Judicial Power for interpretation of the legislation in order to secure equal application of the legislative rules by the national courts.

The questions brought for interpretation were (1) if importation of original goods without the consent of the proprietor, where the trademark is affixed to these goods with the consent of the proprietor, constitute infringement of article 73, (1)<sup>21</sup> in relation to article 13, (2), point 3<sup>22</sup> of the Law on the Trademarks, as

---

20. Interpretative Decision 1/2008 of June 15.

21. Art. 73. (1) Any person who, in his business activity, uses a sign as provided in Article 13 without the consent of the proprietor thereof shall be regarded as an infringer.

22. Rights Conferred by a Mark.

Art. 13. (1) The right in a mark shall comprise the right of its holder to use it and dispose of it, and to prevent third parties not having his consent from using in the course of trade:

(i) any sign which is identical with the mark in relation to goods or services which are identical with those for which the mark is registered;

(ii) (suppl. - State Gazette No. 43/2005, in force since 21.08.2005) any sign where, because of its identity with or similarity to the mark and the identity or similarity of the goods or services covered by the mark and the sign, there exists a likelihood of confusion on the part of the consumers; the likelihood of confusion includes the likelihood of association between the sign and the mark;

(iii) (amended - State Gazette No. 43/2005, in force since 21.08.2005) any sign which is identical with or similar to the mark in relation to goods or services which are not identical with or similar to those for which the mark is registered, where the earlier mark has a reputation in the territory of the Republic of Bulgaria and where use of that sign without due cause would take unfair advantage of, or be detrimental to, the distinctive character or the repute of the earlier mark.

(2) (amended - State Gazette No. 43/2005, in force since 21.08.2005; amended - State Gazette No. 73/2006, in force since 06.10.2006) For the purposes of paragraph (1), "using in the course of trade" means:

(i) affixing the sign to the goods or to the packaging thereof;

(ii) offering the goods, placing them on the market or stocking them for these purposes under that sign, or offering or supplying services thereunder;

(iii) importing or exporting the goods under that sign;

(iv) using the sign on business papers and in advertising.



first question and (2) when trademark rights should be deemed exhausted – at the time of putting on the market by the proprietor or with his consent of good from the same type for which the trademark is registered or after putting on the market of each one particular good?

According the Supreme Court of Cassation the controversy in practice of the national courts could be found in the existence of two opposite interpretations:

Some of the courts rule that importation of goods without the consent of the proprietor does not constitute infringement of article 73, (1) in relation to article 13, (2), iii. These courts would interpret the Law on Trademarks in a way that an infringement under article 73 of the Law should be applied in strict relation to the rule of article 13, (1) and to be namely established if the goods are not original (if the sign is not been affixed by the proprietor or by third party with his consent). On the other hand, some of courts would find an infringement in the case of import of original goods grounded on the lack of consent of the proprietor, interpreting article 13 of the Law in a way that rules (1) and (2) are regulating different cases of infringement. These courts would consider the originality of the goods irrelevant for the infringement.

The Supreme Court first discussed the specific subject matter of the protection against infringement of trademark rights established by the Law on the Trademarks. It came to the conclusion that under the special rules of the Law on Trademarks the protection against infringement is limited as to the prohibition established for the use in the course of trade by third parties without the consent of the proprietors of a sign that is identical or similar to the trademark for identical or similar goods, and that any infringements related to the exercising of the rights of the proprietor to use and to dispose the trademark are subject matter of protection of the civil and commercial legislation. According to the Supreme Court, the actions provided by the Law on Trademarks for protection of the proprietor are in force only in case of lack of consent on behalf of the latter for the use of identical or similar sign (affixing the sign to the goods). Then the Court defined that the essential function of the trademarks is to serve as signs capable of designating the goods or the services of certain entity and distinguishing them from the goods or services of other entities, thus providing guarantees for the consumers as to the identity and source of origin of these goods or services and preventing the of likelihood of confusion on behalf of the consumers.

Based on the above assumptions the Court established that whenever original goods are being traded on the market, it will be with the consent of the proprietor and the latter will not be entitled to the actions provided for protection in the case of infringement under article 73 of the Law (as it only includes cases of non original goods). According to the Court the protection can be relied upon

circumstances where the sign or its copy have been affixed to the goods by third party without the consent of the proprietor, as the consent under article 13 is such regarding the designation of the goods. Thus the Court actually adopted the principle of worldwide exhaustion of the trademark rights without referring to the rule for the exhaustion. Interpreting the rule of article 15 of the Law<sup>23</sup> on Trademarks for the exhaustion of the rights conferred upon the registration, the Supreme Court came to the conclusion that it is irrelevant to the liability established under article 73 of the Law. The arguments here were that article 73 from the Law made no reference for infringements to the exhaustion rule of article 15, but only to article 13 and as a norm that imposes sanctions it cannot be widened in its interpretation.

Finally the Court stated that in cases of parallel importation of original goods, the proprietors should seek protection for their non exhausted rights on the grounds of contractual or non contractual liability against the third parties that import the original goods but not to rely on the special protection under article 73 of the Law. Thus, answering the question of the Chairman, the Supreme Court of Cassation interpreted the Law on Trademarks in a way that an import of original goods where the trademark has been affixed by the proprietor or with his consent does not constitute infringement of the trademark rights under article 73 (1) in relation to article 13 (2), iii.

## ***2.2 Sofia City Court brings the issue to the Court of the EU***

The decision of the Supreme Court did not succeed to calm down the spirits. There were negative reactions mostly on behalf of the industries which rights were affected. There were also some critical reviews from professionals<sup>24</sup>. In fact the decision itself was far from unanimous as five of the judges, including the Chairman, did not support it. The courts, regardless that they were obliged to follow that interpretation on their side found it controversial to the EU Directive and to the decisions of the Court of the EU.

The saga continued within a case brought at the Sofia City Court (Sofiyski gradski sad) by Cannon claiming infringement based on unauthorized import in Bulgaria of some toner cartridges. The goods were purchased in a country outside the EU

---

23. Art. 15. (1) (amended – State Gazette No. 73/2006, in force since the date of Accession of the Republic of Bulgaria to the European Union) A mark shall not entitle the proprietor to prohibit its use in relation to goods or services which have been put on the market in the territory of the European Union member states, respectively of the European Economic Area, under that mark by the proprietor or with his consent.

24. Politov, Yordan (2010), The Exclusive Trademark Right and the Parallel Imports, *Sobstvenost i pravo*, No 5, pp. 79-94.

and then the buyer shipped them to the port of Bourgas in Bulgaria, but border measures were taken against him. The Sofia City Court allowed as security measure seizure of the products which was appealed by the buyer and confirmed by the Appellate Court. Cannon then started proceedings before the Sofia City Court claiming infringement of its exclusive rights by the buyer. Under the Law on Judicial Power, the Court had to apply the interpretation of the Supreme Court of Cassation. Still Sofia City Court decided to stop the proceedings and refer to the Court of the European Union for a preliminary ruling for interpretation of article 5 in relation to article 7 of First Directive submiting the following question<sup>25</sup>:

“Is Article 5 of First Council Directive 89/104/EEC 1, in so far as it confers on the trade mark proprietor the exclusive right to prevent all third parties not having his consent from using in the course of trade any sign which is identical with the trade mark, for example importing or exporting goods under the sign, to be interpreted as meaning that the trade mark proprietor’s rights include the right to prohibit use of the trade mark without his consent through the importation of original goods, provided that the trade mark proprietor’s rights under Article 7 of the directive are not exhausted?”

The Court of the EU issued an Order on the 28th October 2010 stating<sup>26</sup> that the answer of this question has already been formulated in previous rulings and applied paragraph 104 (3) from the Rules of Procedure of the Court of Justice<sup>27</sup>. A number of rulings were cited by the Court, first to be *Class International* (C-405/03, paragraph 58) where the Court held that “if the offering or the sale necessarily entails putting goods bearing the mark on the market in the Community, the exclusive rights conferred on the proprietor of that mark by Article 5(1) of the Directive and Article 9(1) of the Regulation have been adversely affected, regardless of the place in which the addressee of the offer or the purchaser is established and irrespective of the provisions of the contract ultimately concluded regarding any restrictions on resale or the customs status of the goods. The offering or the sale is then ‘using [the mark] in the course of trade’ within the meaning of Article 5(1) of the Directive and Article 9(1) of the Regulation. It follows

---

25. Reference for a preliminary ruling from the Sofiyski gradski sad (Bulgaria) lodged on 18 November 2009 - *Canon Kabushiki Kaisha v IPN Bulgaria* (Case C-449/09), <<http://curia.europa.eu>>, accessed 29.03.2011.

26. Order of the Court (Fifth Chamber) of 28 October 2010, (Case C-449/09).

27. Where a question referred to the Court for a preliminary ruling is identical to a question on which the Court has already ruled, or where the answer to such a question may be clearly deduced from existing case-law, the Court may, after hearing the Advocate General, at any time give its decision by reasoned order in which reference is made to its previous judgment or to the relevant case-law.

that the trade mark proprietor may oppose it pursuant to Article 5(3)(b) of the Directive and Article 9(2)(b) of the Regulation". Following the Court stated that it is within the competence of the national jurisdiction to establish where in the particular situation the importer personally or through a third party intended to put the goods on the EEA market (paragraph 20). As for the interpretation of the national legislation in relation to the European Union law the Court referred to the *Silhouette International Schmied* (C 355/96), where in paragraph 26 of the Decision it held that: "...the Directive cannot be interpreted as leaving it open to the Member States to provide in their domestic law for exhaustion of the rights conferred by a trade mark in respect of products put on the market in non-member countries." Further in paragraph 23 of its Order, the Court held it has been already established in consecutive decisions that the exhaustion is limited only to cases of putting of the goods on the market within the European Economic Area, thus allowing the proprietor to exercise control over the initial marketing of the goods in the EEA (*Zino Davidoff*, C 414/99—C 416/99, *Van Doren* C-244/00, paragraph 26, and *Peak Holding*, C-16/03, paragraph 36).

The Court then stated in paragraphs 24 and 25 that when the goods were not put on the market by the proprietor or with his consent, the latter will be entitled to prevent any third party from importing these goods (*Peak Holding*, paragraph 34) and that following the established practice of the Court, in the case where the national jurisdiction reaches a conclusion that the importer is intending to put the goods on the market or sells the goods to a third party that will necessarily entail putting them on the market of EEA, then it will constitute first putting on the market of original goods without the consent of the proprietor and the court practice referred above should be applied.

Finally, the Court of the EU answered the question of the Sofia City Court that article 5 of the Directive must be interpreted "as meaning that the trade mark proprietor may oppose the first placing into circulation in the course of trade in the European Economic Area, without his consent, of original goods bearing that mark".

### ***2.3 Back to the beginning***

Thus, the decision of the Supreme Court of Cassation was de facto "overruled" by the Order of the Court of EU and has not to be followed by the national courts in Bulgaria. The Order of the Court of EU left no doubt on the interpretation of article 5 of the Directive, and the principle of the primacy of the European Union Law obliges the Bulgarian courts to give priority to it before any internal acts including the decision of the Supreme Court of Cassation. But these two rulings bring to front some important issues. At first it was made clear that the courts in Bulgaria are well acquainted to the EU legislation and to the practice of the Court of the EU. Through its request to the Court of EU, the Sofia City Court found its

way to decide in compliance to the established practice of the Court of EU regardless the binding interpretation of the Supreme Court of Cassation. Secondly, it is also evident that the problem is more than interpreting the legislation, but rather driven by the function of the trademarks to serve as indication of the origin of certain goods or services.

In its decision<sup>28</sup> the Supreme Court underlined that an essential characteristic of a trademark is to establish guaranties to the consumer regarding the identity of the origin of certain goods that would enable the latter to recognize these goods and to avoid confusion to goods that are with different origin. In regard to the liability of the third parties provided under the Law of Trademarks, the Court refused to treat in the same way cases where the sign is affixed to the goods without the consent of the proprietor and cases where goods are original. It made reference to the civil legislation and to the Consumer Protection Act as laws establishing the relevant legislation that would provide special legal actions for protection of the proprietor against infringement by his contracting parties<sup>29</sup>. The Supreme Court also stated that the legislator has adopted different means for protection in cases where goods are original, and in cases where they are not on the other hand and that the protection against infringement of original goods should be based on the rules of the contractual or non contractual civil liability.

Indeed, it could hardly be defended that piracy and counterfeiting and parallel imports are two cases of infringement to which the same remedies should be applied. Such kind of general and broad interpretation has soundly been criticized as inappropriate<sup>30</sup>. It has been also reasonably argued that under article 13 of the Law on Trademarks the fact of infringement does not include cases where the goods are original<sup>31</sup>. An established principle under the Bulgarian law, sanctions can be imposed only for the explicitly defined by the legal acts cases. Just on the contrary, following the EU exhaustion doctrine, the Law on Trademarks appears to provide sanctions for an act that is not itself defined as an infringement. The bare fact of non exhaustion of the trademarks rights does not constitute infringe-

---

28. Supra note 21, Paragraph 3.

29. Supra note 21, Paragraph 6.

30. Kur, Anette, (2008) Fundamental concerns in the harmonization of (European) trademark law, *Trademark Law and Theory*, pp 151-177, p. 172, The author discusses a proposal for a directive on criminal remedies. For infringement and the trends to broaden the scope of trademark protection to the extent that "virtually all modes of trademark use fall under its provisions".

31. Markov, Emil (2009), *The Principle of Exhaustion of Trademark Rights*, pp. 293 – 334.

ment<sup>32</sup>. Therefore, it is indeed not well founded to apply one and the same rules for counterfeiting and parallel imports.

Another important issue is the one related to the consent of the proprietor for first placing of the goods on the market. The consent has been a milestone in the establishment of the EU exhaustion doctrine. The problem here occurs as different national laws and practice have developed different concepts on the consent<sup>33</sup>. In some States the consent for re-sale of goods designated by a trademark will be deemed to be implied into the act of first sale unless otherwise specified, while in other countries the consent should be given explicitly by the proprietor. On the other hand receiving the explicit consent sometimes seems to be practically infeasible as the goods in question might have been sold numerous times before been purchased by the parallel importer. Under the Bulgarian trademark legislation there is no specific rule defining the consent for re-sale of branded goods, the latter should be deemed to be implied within the act of the first sale under the general rules of the civil law. To overcome these differences between the states the issue has been decided by the Court of the European Union in a way that consent should be explicitly given<sup>34</sup>. Resulting from the above both states where the exhaustion was based on the implied consent doctrine (Great Britain) and states where the world wide exhaustion of rights was applied with the explicit consent needed (Germany), reach the very same end, namely exhaustion limited to the EU and EEA countries and consent expressly given at the time of the first sale.

The ruling of the Supreme Court of Cassation is just another indication for the need of finding a different solution. Problems arise in relation to national substantive and procedural laws, free movement and competition rules and even the WTO law<sup>35</sup>. The EU exhaustion of rights does not fit two essential concepts, namely the function of the trademark to designate the origin of the goods or the services and the world wide exhaustion applied to other intellectual property

---

32. Supra note 32. The author also refers to the second answer of the Court in the *Silhouette Case* (C-355/96) .2. Article 7(1) of Directive 89/104 cannot be interpreted as meaning that the proprietor of a trade mark is entitled, on the basis of that provision alone, to obtain an order restraining a third party from using his trade mark for products which have been put on the market outside the European Economic Area under that mark by the proprietor or with his consent."

33. Thomas Hays, (2008) *The free movement (or not) of trademark protected goods in Europe*, trademark law and theory, 204-229, page 219

34. *Zino Davidoff v A&G Imports*.

35. Herman Cohen Jehoram, (1998) *International exhaustion versus importation right: a murky area of intellectual property law*, GRUR International 1996-4, 280-284.

rights. Besides that in certain cases it results in imposing sanctions such as for counterfeiting for the sales of original goods. It seems that if anyone benefits it will not be the consumer, but rather the proprietor. And though there is nothing wrong for the proprietor to increase its profits should it be done by means of the trademark legislation and at the expense of the consumers?

### Concluding remarks

Trademark legislation and practice in Bulgaria Face the challenges of the membership in the European Union. The spread of the CTM system over the Bulgarian territory led to decrease of the national applications for registration of trademarks. The switch to the opposition based registration may soften that effect to a certain extend at least in regard to cutting the terms of the registration process. On the other hand, EU rules are now applied and followed by the national courts. Still Bulgaria's courts seem not to be an exception when it comes to interpretation of exhaustion of rights in relation to parallel imports. This has been one of the biggest issues of the national court disputes in the recent years. This situation resulted in a decision of the Supreme Court of Cassation that made the Court of EU to confirm again what it has ruled in its previous decisions. It is indicative that for the Supreme Court parallel imports and counterfeiting should be treated differently. The decision brought to front the consumer's interests and underlined the essential function of the trademarks to serve as indications of origin. Once more the need of another solution has been demonstrated. Possible answers have been already been given<sup>36</sup>, namely adoption of world wide exhaustion principle and territorial restrictions by contracts. After all, if the function of the trademark is to designate the origin, then once the original goods are placed on the market, "a trademark right in a product can comfortably end"<sup>37</sup>.

---

36. Supra note 32, supra note 36.

37. Supra note 34, page 227.

# Can the EU's data protection rules survive data transfers to third states?

---

---

Els De Busser

---

---

## 1. Introduction

Globalisation is the word on everyone's lips in the 21st century, going from marketing and advertising, to educating, to investigating, detecting and prosecuting criminal offences. Recognising the international scale of criminal offences – either committed through the means of information technology, either through using a network of contacts in a number of states – national judicial and law enforcement authorities have increased their mutual cooperation and international agencies assigned to coordinate and facilitate this cooperation have been established.

Multilateral and bilateral mutual legal assistance instruments that regulate the key feature in judicial and law enforcement cooperation in criminal matters, the exchange of information, usually do not include detailed provisions on the protection of personal data. When the mutual cooperation involves only EU Member States, all are bound by the same data protection principles because all Member States have ratified the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of 1981 (further: Data Protection Convention).

When third states (states that are not Member States of the EU) cooperate with a Member State, there are two possibilities: the third state has also ratified the Data Protection Convention or it has not. In case of ratification of the Data Protection Convention, the requested Member State can safely assume that the requesting third state will process the personal data adequately, i.e. in compliance with the data protection principles that it adheres to. In case of a third state that has not ratified the Data Protection Convention, several scenarios could occur. The third state could have a data protection regime that is similar but not equal to a regime that complies with the Data Protection Convention or it could have a legal framework that is based on fundamentally different data protection principles. It could even have no data protection rules at all. This is where the *adequacy requirement* comes in, i.e. the requirement for a Member State or the European Commission to assess the level of data protection in a third state to which personal data should be transferred.



The EU and not the Council of Europe, was the first to introduce the requirement of an adequate level of data protection. In Directive 95/46/EC, the EU laid down the rules for exchanging personal data within the scope of European Community activities (including commercial trade). Due to this particular scope which essentially reaches beyond the external borders of the EU, the Directive also provided in rules on data protection when doing business with third states. Art. 25 of the Directive requires an assessment of the adequacy of the level of data protection in the third state.

As the first provision in its kind for the EU, the adequacy requirement ruffled a few feathers in third states' authorities. Before the Directive was even adopted, reactions surfaced on how this would affect the trans-border flow of data such as payments made electronically in international trade. (Boehmer and Palmer, 1993; Raab and Bennet, 1997; Long and Quek, 2002) The first effect of the requirement of an adequate level of data protection was felt in the US, resulting in the so-called Safe Harbour compromise. This compromise was a set of data protection rules the US promised to apply when receiving data from an EU Member State.

In 2001 the Council of Europe included the adequacy requirement for *all* automatic data processing in its Additional Protocol to the Data Protection Convention. In the area of judicial and law enforcement cooperation in criminal matters, the transfer of data to third states has been protected by the adequacy requirement in the Europol Decision, the Eurojust Rules of Procedure and the Framework Decision on data protection in criminal matters in 2008.

The US has a special relationship with the EU. The EU presidency representing the Member States, but also Eurojust and Europol, entered into negotiations with the US in order to regulate the exchange of personal data. These data transfers were deemed necessary for the purpose of prevention, investigation and prosecution of criminal offences. The heightened need for mutual cooperation between the two resulted in concluding a number of agreements and negotiating several more at the moment. This contribution will deal with the cooperation in criminal matters with third states in general. However due to the amount of agreements with the US in this area and the intensity of the negotiations, the EU's relationship with the US will form a significant part of this text, especially with regard to the adequacy requirement.

First, the requirement for an adequate level of data protection will be clarified, followed by the difficulties in fulfilling this requirement. Subsequently, the agreements between the EU, Europol, and Eurojust, on the one hand, and third states on the other hand, will be scrutinised with regard to their compliance with the adequacy requirement. Heightened attention will be paid to the US in this respect. Finally, the future of the adequacy requirement will be studied as the

European Commission aims to clarify and simplify the assessment of an adequate level of data protection in its 2011 comprehensive approach on data protection.

## 2. Why an adequacy requirement?

The Data Protection Convention has a general scope including all automatic processing of personal data and its data protection principles have been formulated wide enough to be valid regardless from time, technological advancement, data processor or type of data. These two characteristics have shaped not only the EU legal framework on data protection but through implementation of EU legal instruments also the data protection systems of all EU Member States and the EU institutions and agencies. For these reasons, the Data Protection Convention has earned the name “umbrella legislation” giving the group of 27 Member States a common foundation concerning data protection. It is the responsibility of the Member State implementing the rules of the Data Protection Convention to make these precise and complete in order to accomplish the goal it is bound by. In transferring data to a state, the distinction should be made as to whether the receiving state is a Member State or a third state.

On the one hand, when personal data are exchanged between authorities within one Member State or between judicial and law enforcement authorities located in different Member States, they are still transferred to a legal system that is bound by the same basic principles on data protection as the legal system they originated from. Obstacles caused by a difference in data protection rules will hardly occur in such cases.

On the other hand, when personal data are located in an EU Member State and transferred to a third state, two scenarios could occur. Firstly, the receiving state could be bound by the Data Protection Convention and thus by the same basic principles governing the EU's data protection regime. Secondly, the receiving state could be a state that did not ratify the Convention. The receiving state could have a different – possibly diverging – view on data protection. The requested personal data could thus be transferred to and processed in a legal framework that offers lower data protection safeguards than the EU Member State from which the data originated. The opposite case – stricter data protection rules in the receiving state – is equally possible, but would not give rise to many difficulties unless the smooth international exchange of data is hindered by applying stricter rules.

Aiming at avoiding the situation in which personal data are transferred to a third state that endorses lower standards of data protection than the EU standards, the Additional Protocol to the Data Protection Convention has laid down the prerequisite of evaluating the level of data protection in a third state before transferring

data. This evaluation means that the receiving state must at least have an adequate level of data protection. The term “adequate” does not imply that the level of data protection has to be equivalent to the EU’s level, nor does it imply that the receiving state needs to utilize also umbrella legislation. It does imply that the EU rules on data protection will not be violated by transferring personal data to another system of rules.

The Additional Protocol does not clarify who should be in charge of the assessment or how it should be done (cf. *infra*). Nonetheless, the Additional Protocol is not the only instrument that lays down the adequacy requirement, even though it is the only one with an all-embracing – umbrella – scope including all personal data that are automatically processed. The adequacy requirement has also been copied in legal instruments that cover a more specific part of personal data processing (cf. *infra*). This underlines the fact that the requirement of an adequate level of data protection has become the basic prerequisite for external transfers – i.e. to a third state – of personal data, at least in theory.

To allow for some flexibility on the part of the states exchanging data, the Additional Protocol allows for derogations from the adequacy requirement that should be interpreted restrictively. Similar to the derogations from the provisions on human rights in the European Convention for Human Rights and Fundamental Freedoms (ECHR), they should at least be laid down by (national) law and be necessary for the protection of legitimate prevailing interests. Corresponding to the ECHR, the explanatory report to the Additional Protocol also refers to the same interests, based on which the right to privacy and data quality principles can be lawfully derogated from as follows: to protect an important public interest, the exercise or defense of a legal claim, or the extraction of data from a public register. Exceptions can also be made for the specific interest of the person whose data are transferred for the fulfillment of a contract with this person or in his interest, to protect his vital interests or if he has given his informed consent.

In case an adequate level of data protection cannot be assured, another possibility for exchange still exists if the receiving state provides sufficient safeguards that are deemed adequate by the requested state. The safeguards can be limited, however, to include only the relevant elements of data protection and are only applicable to a specific transfer of data.

### 3. The paradoxical adequacy requirement

The requirement of an adequate level of data protection is meant to safeguard the EU rules on data protection and aims at offering citizens a similar level of protection in case their personal data are sent to an authority located in a third state. Third states can have different rules on data protection that are contrary to the

legal framework endorsed by the EU, meaning that the EU rules would be violated when transferring data to that third state. For example the rule that personal data may only be gathered for a specific purpose and may not be processed for a purpose that is incompatible with the original purpose, is a rule that does not exist in its general form in the US data protection regime. On the contrary, US legislation provides in an exemption of the rule that no personal data can be disclosed without the consent of the data subject that is called "routine use" (5 USC §552a(a)(7)). This means that US agencies such as the FBI can disclose personal data when they deem the disclosure to fall within the scope of what they themselves define as a routine use. In the case of the FBI the disclosure of data during appropriate legal proceedings was called a routine use (De Busser 2009, p. 266).

Safeguarding the EU's data protection rules is therefore a significant objective and the prerequisite of an adequate level of data protection in the receiving state could be expected to be at least a uniform requirement for all outgoing data transfers and transparent in its meaning as well as its method. Especially with regard to the sensitive area of criminal investigations and prosecutions, assessing the legal framework within which the requested data would be processed seems a substantial step to take before agreeing to a transfer.

Nevertheless, when studying the rules governing data protection in external transfers and the adequacy requirement, it can not be ignored that firstly, a number of inconsistencies exist and secondly, several questions remain unanswered. The inconsistencies are caused by the fact that the importance and substance of the adequacy requirement are diametrically opposed to the sloppiness with which it was laid down in legislation. Differences in rules and differences in the applying of these rules are the result. Questions that remain unanswered relate to the authority that should determine the adequacy of a data protection system and which items should be included in the assessment.

## **1. Rules that are inconsistent**

In spite of its importance and substance, the adequacy requirement is governed by rules that lack consistency. The inconsistency lies first of all in the fact that an adequacy assessment is not mandatory for all data transfers to third states. Secondly, the fact that authorities responsible for the cooperation in criminal matters show substantial differences in their methods of assessing adequacy is a feature that is contrary to legal certainty. This shows inconsistency in rules that have the same objective. Thirdly, in cases where it is mandatory to evaluate third states' legal framework on data protection, this obligation is not always complied with. Unjustified distinctions are made between third states which may lead to political or diplomatic difficulties.

### ***Not mandatory***

Even though the aim of the requirement is the same for every outbound data transfer, i.e. the safeguarding of the EU's legal framework on data protection, the rules are not the same. A fortiori, the prerequisite of an adequacy assessment is not a prerequisite for every transfer of data to a third state. Depending on the requested Member State, the requested EU body and the purpose data are processed for. These three characteristics result in a diverse picture regarding the adequacy requirement, a picture that is conflicting with the substance and importance of the assessment.

Firstly, the Additional Protocol that has laid down the adequacy requirement for all data processing by automatic means has so far been ratified by 19 EU Member States. In spite of its general scope, the partial ratification of the Protocol means that the adequacy requirement is not a uniform requirement for all data transfers from the EU to third states. Besides creating a pattern of different conditions on data transfers depending on which Member State they originate from, the lack of a uniform adequacy requirement also creates the risk for *data-shopping* or the search for the most lenient data protection regime. When a third state does not become the requested data due to a negative adequacy evaluation, it could rely on a Member State that is either willing to decide positively on the adequacy assessment or is simply not bound by the requirement in the first place.

Secondly, since eight Member States have not ratified the Additional Protocol, there is no general legal instrument that is binding for all Member States and provides in the adequacy requirement. There are however EU legal instruments that are binding for all Member States and provide in the adequacy rule, yet have a limited scope as they are only applicable to a specific group of data transfers. In the pre-Lisbon Treaty era, when the former pillars still determined the scope of the legal instruments, data processing for the purpose of Community activities were governed by Directive 95/46/EC. Data processing in the electronic communication sector is covered by Directive 2002/58/EC that complements the provisions of Directive 95/46/EC. In addition, the data processed and transferred between the Community institutions and bodies and by these institutions and bodies to third bodies are regulated by Regulation 45/2001, which also includes the adequacy requirement for sending data to third bodies. Directive 95/46/EC is the most important of these legal instruments as it covers commercial activities and thus has significant economic repercussions. The Directive applies the data protection principles of the Data Protection Convention for Community activities and widens their scope to also include non-automatic processing of data.

The European Commission recognized in its 2011 comprehensive approach on data protection that the Directive needs to be reviewed in function of techno-

logical advancement. The basic data protection principles are still valid, but the adequacy requirement needs to be clarified and simplified. This goes for the adequacy requirement in general, not just the provisions on adequacy laid down in the Directive.

Finally, data processing for the purpose of investigation, detection and prosecution of criminal offences was regulated by the 2008 Framework Decision on data protection in criminal matters. Also this Framework Decision provides in an adequacy requirement for transfers to third state authorities. Nevertheless, the scope of the Framework Decision only includes personal data that a Member State has received from another Member State, either by a transfer of data or by means of an information system.

The particular scope of all these legal instruments implies that even when studying the instruments that are not dependent on ratification but binding for all Member States, no generally applicable adequacy rule can be detected. In fact there are only two cases in which all Member States must make an adequacy assessment. The first case is that in which the processing of personal data falls within the scope of Community activities and is thus ruled by Directive 95/46/EC. The second case concerns the processing of personal data that the transferring Member State received from another Member State and is transferring for the purpose of a criminal investigation.

### ***Not uniform***

Both Eurojust and Europol can conclude cooperation agreements with third states. In as far as these agreements include the transfer of personal data to third states; the adequacy requirement should be complied with as both bodies have incorporated the adequacy test in their own respective rules on data protection. Since both Europol and Eurojust perform tasks in coordinating and facilitating law enforcement respectively judicial cooperation in criminal matters and therefore also cooperate and exchange information (including personal data) with each other, one would expect that both have at least a similar method for protecting data that are transferred to a third state. This is not the case.

Eurojust, the EU's judicial cooperation body, has laid down its detailed rules on the protection of personal data in its Rules of Procedure on the Processing and Protection of Personal Data at Eurojust (further: Eurojust Rules). The Eurojust Council Decision as amended in 2008 allows Eurojust to conclude agreements with third states providing in personal data transfers after consultation of the Joint Supervisory Body and approval by the Council. For transfers to third states the Eurojust Rules mention the Data Protection Convention. For transferring personal data to parties to this Convention, the adequacy assessment is obviously

not needed. With regard to transfers of personal data to third states, the Eurojust Rules provide in an adequacy assessment by the body's own data protection officer. This assessment is followed by a decision taken by the national member(s) who are involved. The Eurojust Joint Supervisory Body intervenes when the data protection officer experiences difficulties in making his adequacy evaluation.

Europol utilizes a more elaborate approach when adequacy assessments are concerned. No less than four steps need to be taken in order to reach a decision on the level of data protection in a third state that Europol wants to conclude an agreement with.

When no urgent circumstances apply, the procedure for reaching an adequacy decision starts with a report by the Management Board stating that no obstacles exist to start negotiations with the third state in question. The Joint Supervisory Body (JSB) is consulted by the Management Board on this subject as well. During this stage, a first check of the third state or data protection system can be made as the JSB protects the rights of the individual regarding the processing of data by Europol. Subsequently, a unanimous decision by the Council of the EU is needed. This means that a second check of the data protection framework is made as the Council should consider the law and the administrative practice of the third state in the field of data protection, including the authority responsible for data protection matters.

In a third stage, the Director starts the negotiations. Finally, the Management Board and the JSB give their approval to conclude the agreement (De Hert and De Schutter, 2008).

When urgent circumstances apply, it is the Director of Europol who decides whether the transfer of data is absolutely necessary to safeguard the essential interests of the Member States concerned within the scope of Europol's objectives or in the interests of preventing imminent danger associated with crime. The adequacy evaluation should in these cases be done by the Director. This means that supervision is limited to a post-transfer check and only if the Management Board and the JSB file a request.

The assessment made by the Director of the third state's data protection framework then substitutes the lengthy four-step process. The Europol Decision only states (Art. 23, §8) that the obligation for the Director to consider the data-protection system of the receiving body in question should be carried out with a view to balance the data-protection level and the interests for the protection of which the transfer is made.

The Europol Decision that replaced the Europol Convention added the obligation for the Director to inform the JSB and the Management Board of the decision

taken and of the basis of the assessment of adequacy. This does not offer a stronger data protection in comparison to the Convention as the Director is still only bound to make a balancing exercise between the data protection level and the interests concerned. The text does not provide that the JSB or the Management Board can undertake any actions and the decision is already made at the time they are informed. Providing in an option of a post-factum check of adequacy as opposed to a prior evaluation, means that in cases where the level of data protection would be considered not to be adequate, this could only affect possible future transfers to that same third state instead of blocking a currently planned transfer.

Even though the Europol Decision has entered into force after the Framework Decision on Data Protection in Criminal Matters, this did not have an effect on the transfer of personal data from Europol to a third state as Art. 13 of the Framework Decision only includes Member States.

It can only be concluded that Europol and Eurojust have very different rules on data protection in transfers to third states. The layered adequacy evaluation system of Europol is without judicial counterpart. Due to the importance of the adequacy requirement – the protection of personal data that are transferred to a state with an unknown data protection level – it is surprising to see such differences between the EU's judicial and the law enforcement body instead of an equivalent evaluation system for Eurojust as has been established for Europol.

The 2008 Framework Decision on data protection in criminal matters did not provide in the adequacy requirement in its draft stage until the European Data Protection Supervisor called for more consistency with the aforementioned Additional Protocol to the Data Protection Convention. In the adopted text, Art. 13, §1, d) lays down the requirement of only transferring data to states that have an adequate level of data protection. The provision is copied from the Additional Protocol. However, due to the limited scope of the Framework Decision, also this adequacy requirement is only mandatory for transfers of data that were received from or made available by a Member State. It does not include data that were collected by the providing Member State itself. In case this Member State does not have an adequacy requirement in its national legislation and did not ratify the Additional Protocol, the transfer can go through without any adequacy assessment whatsoever.

Copying the provisions on adequacy from the Additional Protocol into the Framework Decision also meant copying the lawful derogations from the adequacy requirement. The reasons for which an authority can lawfully derogate from the adequacy rule are formulated as alternatives to each other. The rule can thus be pushed aside by "legitimate prevailing interests, especially important public interests". Based on its origin in the Additional Protocol to the Data Protection Con-



vention, the legitimate prevailing interests should refer to Art. 8, § 2 of the ECHR and Art. 9, §2 of the Data Protection Convention. That would mean that the term includes state security, public safety, health and morals and the economic well-being of the state. Obviously, these leave plenty of room for more specific interests of the state to fit in one category or the other. Specifically the interests of state security can – nevertheless legitimate and prevailing – cause personal data that were originally gathered for criminal purposes to be processed for administrative purposes, while jumping over the adequacy requirement. This amounts to releasing the data into a legal system of which the data protection provisions are possibly not adequate in comparison to the EU standards.

The derogations to the adequacy requirement in general and the provision on legitimate prevailing interests in particular, are in need of further clarification. This could be done by means of an exhaustive list, a supervisory authority that judges the legitimacy and the prevailing force of a specific interest or by laying down common standards on when to consider an interest as prevailing over the adequacy assessment of a data protection system.

### ***Not applied***

The adequacy requirement may not be mandatory in all cases of outbound data transfers, the cases in which it is mandatory, this authority is also obliged to comply with it. Nevertheless politically more opportune choices could prevail. Studying the cooperation agreements concluded between the EU, Eurojust and Europol on the one hand and a third state on the other hand, there is a clearly different approach when that third state is the US. In the case of the EU representing its Member States and concluding agreements on behalf of them (former Arts. 24 and 36, current Art. 216 TFEU), there are three examples: the 2003 Agreement on Mutual Legal Assistance in Criminal Matters between the EU and the US (2003 EU-US MLA Agreement), the 2010 Agreement on Mutual Legal Assistance in Criminal matters between the EU and Japan (2010 EU-Japan MLA Agreement) and the 2010 Agreement between the EU and the US on the processing and transfer of Financial Messaging Data from the EU to the US for the purposes of the Terrorist Finance Tracking Program (2010 TFTP Agreement). In the case of Eurojust and Europol, both have concluded cooperation agreements involving the transfer of personal data with many third states.

### ***Unclear mandatory nature***

The first question is whether the adequacy assessment was mandatory in concluding these agreements. As mentioned earlier, both Eurojust and Europol are bound by the adequacy requirement. They are not parties to the Additional Protocol to the Data Protection Convention, but have included the requirement in their

own set of rules governing their data transfers to third states. Whether the EU presidency in its role of representing the Member States is bound by the requirement is a more difficult question to answer.

The 2003 EU-US MLA Agreement was concluded when there was no data protection legal instrument in the EU for the former third pillar. Since the Agreement focused on criminal matters the only other reason for assessing the level of data protection of the US would be the Member States that ratified the Additional Protocol to the Data Protection Convention. At the time of signing the 2003 EU-US MLA Agreement 14 Member States were bound by this Protocol and thus by the adequacy rule. This could have been sufficient reason for the European Commission to make an adequacy assessment before the presidency concluded the Agreement with the US authorities. This was not done. In fact, the text of the Agreement does not even allow an adequacy check as it forbids all “generic restrictions” that can hinder the smooth flow of information. Generic restrictions can certainly be understood as general requirements to data transfers such as the adequacy requirement. This means that 14 Member States are in fact violating their own data protection rules unless they make their own assessment.

By the time the 2010 EU-Japan MLA Agreement was signed on 15 December 2009, 16 Member States had ratified the Additional Protocol. The 2010 TFTP Agreement was signed on 28 June 2010, which means that 17 Member States were at that time bound by the Additional Protocol. Nevertheless there now was a genuine legal basis for the adequacy check since the former third pillar had received its data protection instrument, the 2008 Framework Decision on data protection in criminal matters. This Framework Decision prohibits Member States of transferring personal data to states that do not ensure an adequate level of data protection. Due to the limited scope of the Framework Decision this is only the case for those personal data that the transferring Member State received from another Member State. Before organising a transfer to Japan of this group of data, the transferring Member State should make an adequacy assessment of Japan’s legal framework on data protection. So far, a decision on Japan’s level of data protection has not been taken.

In general, it still unclear whether adequacy assessments should be made by European Commission or by the Member States (cf. *infra*). Thus, in the case of the EU concluding an agreement with a third state, especially when it concerns criminal matters, it would be the most efficient solution for the Commission to make an adequacy assessment on which all Member States can rely in case they want to transfer personal data to a state such as Japan or the US.

In the 2010 EU-US TFTP Agreement, a different approach was used as the Agreement is based on the assumption that the US Department of the Treasury’s

(UST) data protection framework is adequate. Art. 6 explains: “*subject to ongoing compliance with the commitments on privacy and protection of personal data set out in this Agreement, the U.S. Treasury Department is deemed to ensure an adequate level of data protection for the processing of financial payment messaging and related data transferred from the European Union to the United States for the purposes of this Agreement.*” Nonetheless, a genuine assessment of the data protection rules the UST is bound by has not been provided yet.

### ***Clear mandatory nature***

The second question is whether the adequacy requirement was applied in the cases in which it was indisputably mandatory. Again, the cases of Eurojust and Europol concluding agreements with third states should be focused on. As mentioned before both bodies have to comply with their own adopted rules on data transfers to third states or bodies.

The 1995 Europol Convention has been replaced by the Europol Decision which entered into force on 1 January 2010. The new legal instrument only brought about minor changes with regard to the rules on outbound data transfers. These data transfers are for Europol embedded in operational agreements while strategic agreements do not involve the transfer of personal data.

The general rule for Europol for organising the transfer of personal data to third states or bodies is still the conclusion of an agreement, after authorisation of the Council and supported by a prior opinion of the Joint Supervisory Body. In exceptional circumstances, the Director of Europol can enter into negotiations without authorisation of the Council or prior consultation with the JSB. The Director has the discretion to determine what defines exceptional circumstances based on the absolute necessity to transmit personal data in order to safeguard the essential interests of the Member States concerned, within the scope of Europol's objectives, or the absolute necessity to transmit in the interest of preventing imminent danger associated with crime or terrorist offences. The Director must in these circumstances consider the level of data protection applicable for the receiving authority in the third state and weigh this against the essential interests. In this case art. 23 of the Europol Decision provides in a list of parameters to consider when deciding on the adequate level of data protection.

An opportunity was a missed here to further develop these parameters into a more detailed checklist. Possibly the Europol parameters could nevertheless form a basis for the Commission's plans to clarify and simplify the adequacy procedure.

Europol's Director started the negotiations for data transfers to the US after the 2001 terrorist attacks (Mitsilegas 2003). Two agreements were prepared but

only one focused on the exchange of personal data and the making of this agreement shows a strange course when the adequacy requirement is concerned.

The agreement on the exchange of strategic – non-personal – data was started under the exceptional procedure by the Europol Director and shortly after inserted into the conventional procedure at the Council meeting on Justice, Home Affairs and Civil Protection. The Director was during this meeting authorised to conclude the agreement on the exchange of strategic information, not including personal data. At the same meeting, Europol was authorised to start negotiations on another agreement that would focus on the exchange of personal data. Obviously, this means that the level of data protection of the US should be assessed in accordance with Art. 18, §1, 2) of the then applicable Europol Convention and in accordance with the rules governing the transmission of personal data by Europol to third States and third bodies. The Council noted during this meeting that a data protection report on the US had been drawn up by Europol. Nonetheless, the JSB stated that Europol did not provide a report on the data protection law and practice in the US and that the JSB was therefore unable to make a conclusion on the level of data protection in the US. On 3 October 2002, the JSB issued another opinion based on practical experiences with the US system and on presentations made during the negotiations. The JSB stated that the Council was in the position to allow the Director of Europol to conclude the agreement, but expressed concerns about the purposes for which personal data would be used after their exchange to the US. Data should not be used for purposes outside the objectives of Europol. These concerns were based on phrases from the “exchange of notes”, documents that the negotiating parties used to explain their points of view but also to widen the scope of the Agreement. The notes are not formally part of the Agreement, but are intended to assist its implementation. Nonetheless, they explicitly state that the data that are exchanged in accordance with the Agreement can also be used for immigration investigations and proceedings and proceedings relating to *in rem* or *in personam* seizure or restraint and confiscation of assets that finance terrorism or form the instrumentalities or proceeds of crime, even where such seizure, restraint or confiscation is not based on a criminal conviction. These types of proceedings clearly go further than the objectives of Europol laid down in the Europol Convention and later the Europol Decision.

Still, without a proof of an adequate level of data protection the 2002 Supplemental Europol-US Agreement on the exchange of personal data and related information was signed on 6 November 2002. An informal explanatory note only reflecting Europol’s view on the 2002 Europol-US Agreement, states that the provisions of Art. 5 of the Agreement on general terms and conditions “would not be used as a legal basis for generic restrictions, but only in specific cases where there was a real necessity.” The phrase “generic restrictions” was already men-

tioned above in the context of the 2003 EU-US MLA Agreement and is here again used for rejecting the adequacy requirement in the cooperation with the US.

Besides the US, Europol has negotiated operational agreements with Australia, Canada, Croatia, Iceland, Norway, and Switzerland. All of these agreements were negotiated after an opinion of the JSB was issued and confirmed by the Council that no obstacles exist to include the transmission of personal data in the agreement. The only exception to this rule so far is the Agreement with the US.

Eurojust concluded seven cooperation agreements with third states: Croatia, former Yugoslavian Republic of Macedonia, Iceland, Norway, Switzerland, Romania, and the US. Eurojust exchanges case-related personal data with third states which includes data on persons who are subject to a criminal investigation or prosecution, victims, witnesses and convicted persons. In case the third state is not a party to the Data Protection Convention, additional safeguards can be agreed upon between the data controller and third state. With the exception of the US, all of the mentioned states have ratified the Data Protection Convention. In accordance with the Eurojust Rules on data protection, this means that an adequacy check needs to be made of the level of data protection in the US. The Eurojust – US Cooperation Agreement was signed in 2006.

As explained above, Eurojust's data protection officer, who is a member of Eurojust's independent Joint Supervisory Body (JSB) decides on the level of data protection in a third state. Only when difficulties are met in this respect, the help of the full JSB is called for. During the negotiations with the US, the JSB preferred not to be involved directly in the process but wanted to be closely informed on the steps and developments made. Since it is the JSB's task to monitor data processing by Eurojust it is surprising that they did not mention the absence of an adequacy assessment but only expressed concerns on the use of data that had been made public regardless of whether the release had occurred lawfully or not. The JSB also did not make any statements on the provision in Art. 9 of the agreement that was copied from the 2003 EU-US MLA Agreement on the prohibition of generic restrictions as a condition for providing evidence or information.

The two questions asked above regarding the mandatory nature of the adequacy requirement on the one hand and the application of the adequacy check on the other hand, should both be answered negatively. It is not clear whether the EU operating under Art. 216 TFEU is bound by the adequacy requirement but it would certainly have been the right choice considering the Member States' ratifications of the Additional Protocol and considering the substance and meaning of the requirement, especially when the investigation, detection and prosecution of criminal offences is concerned. The mandatory nature of the adequacy assessment is thus not crystal clear. In those cases where it is clear that there is an

obligation to *a priori* evaluate a third state's data protection framework, it is not applied in the agreements covering cooperation in criminal matters with the US. Since it is applied in the relations with other third states, this observation is a clear sign that in the transatlantic relations data protection is pushed aside in favour of uncomplicated data transfers.

## 2. Unanswered questions

Differences in rules relates to the question of mandatory or optional adequacy evaluations and the method used for these assessments. Is the requirement of making an adequacy assessment of a third states' data protection regime an obligation for *all* personal data transfers or not? This question can not be answered by a simple yes or no, but is dependent on the transferring authority, the purpose data are processed for and the ratification status of the aforementioned Additional Protocol. In addition, the question what should be considered while assessing a state's level of data protection, is also still open. When making a comparison between two states' legal systems, does one rely only on "law in the books" or should the application of the law in practice – by means of jurisprudence, decisions by data protection authorities, etc. – also be an element to take into account? Because both questions are intertwined, they are reflected upon here together.

The Additional Protocol lays down that assessments of the level of data protection offered by a receiving third state should be made and when derogations from this rule are allowed, but does not specify which authority should carry out the assessment or how this should be done and what should be included.

The EU legal instruments on data protection allow adequacy evaluations made by the Member States and the European Commission and it is not entirely clear in which cases which authority should make the assessment. Directive 95/46/EC mentions both options while the 2008 Framework Decision on Data Protection in Criminal Matters only mentions a check by the Member States. The advantage of the Commission making the assessment is obviously one uniform decision on a third states' level of data protection on which all Member States can rely. A significant disadvantage of these "block authorizations" is the possibility that the Commission's verdict could be governed by "wider political and economic concerns". (Raab & Bennett 1997) When scrutinizing the transatlantic cooperation agreements and the treatment of the adequacy requirement in that respect, it seems that wider political concerns are also a threat when the EU Member States – represented by the EU presidency – are negotiating an agreement on data exchange with the US.

Member States making their own assessments can lead to different conclusions in different states and create confusion. Due to the lack of uniform rules on the carrying out of the evaluations, Member States could apply diverging methods or could include different items. The case where one Member State includes also the practical application of data protection legislation in the assessment, while another only relies on “law in the books” is not unimaginable. The concern regarding divergent implementation laws in the Member States was also confirmed by the European Commission in its first report on the implementation of Directive 95/46/EC that provides in the adequacy requirement in its Arts. 25 and 26. Recently this has been confirmed again by a study of the national legislations.

In addition, third states could abuse this situation and aim for the Member State that is willing to label their data protection framework as adequate. In that way a third state could receive data that the transmitting Member State received from another Member State – or from a database set up among the Member States – and avoid requesting transfers from a Member State that might not be willing to give a positive adequacy evaluation. From the point of view of the third state requesting personal data from two states, this can cause *data-shopping*. Another concern with Member States making the adequacy assessment is that the national authorities will evaluate a third states’ data protection regime from the point of view of their own national legislation. Even though the national legislations are implementations of EU legal instruments, they can still differ considerably. (Raab & Bennet, 1997)

This is an issue that was also highlighted by the European Commission in its latest strategy on data protection of 2011 as well as by the European Data Protection Supervisor and academics (Raab & Bennett, 1997). The Commission recognized the problem and stated that “*there is a general need to improve the current mechanisms allowing for international transfers of personal data, while at the same time ensuring that personal data are adequately protected when transferred and processed outside the EU and the EEA*”. Therefore, the Commission has made it a goal to not only clarify the adequacy procedure and better specify the criteria and requirements for assessing the level of data protection in a third country but also to make the procedures for international data transfers more coherent.

According to the Explanatory Report to the Additional Protocol, the provisions of Chapter II (basic principles of data protection) of the Data Protection Convention should be taken into account when assessing the adequacy of the third state’s legal framework on data processing. Nonetheless, this clarification is only valid as far as the Convention’s principles are relevant for the specific case of transfer. Thus, the basic principles of data protection do not necessarily have to be considered for every data transfer.

### 3. An attempt to answer some questions

#### *Minimum elements of an adequate level of data protection*

The art. 29 Working Party (hereinafter: 29 WP) is the EU's independent Advisory Body on Data Protection and Privacy established by art. 29 of Directive 95/46/EC. It consists of representatives of the data protection authorities of the 27 Member States joined by the European Data Protection Supervisor and a representative of the European Commission. Its tasks are to provide expert opinion to the Commission on questions of data protection; to promote the uniform application of the data protection principles; to advise the Commission on Community measures affecting individuals' data protection and privacy and make recommendations in this field to the public and to Community institutions. Thus the 29 WP is also the authority that advises the Commission on the adequacy of the level of data protection in a particular third state.

The 29 WP already examined the content of an adequacy assessment in 1997 and published a non-binding discussion document on the central question of adequacy in the context of Directive 95/46/EC. This document and the opinions expressed in it are not applicable to the field of criminal matters. However, assessing adequacy is similar in commercial matters as in criminal matters, although not identical due to the additional rights granted to an individual suspected of a criminal offence and the time pressure as well as the secrecy that is inherently connected to a criminal investigation. Because the document provides guidelines on what an adequacy assessment should include, it can certainly function as a basis for developing ideas on the content of an adequacy assessment in criminal matters.

In addition, the 29 WP identifies three types of data transfers within the scope of Directive 95/46/EC: a transfer between an EU-based data controller and a data controller based in a third state; a transfer between an EU-based data controller and a data processor based in a third state who processes the data on behalf of the data controller, and a transfer between an EU-based data subject and a data controller based in a third state. In the field of personal data transfers in criminal matters, the first type of transfer is the most common one, as these exchanges are organized between law enforcement and prosecution authorities of different states. Data are thus transferred from an authority that determines the purpose and means of processing the data to an authority that has the same competence, yet within a different state and a different set of data protection rules.

As mentioned above, the Europol Decision has also provided in a short list of parameters to consider when evaluating a third state's level of data protection. Because of the scope of the Europol Decision – not including commercial matters



– the list in art. 23 includes elements of data processing rather than the principles governing data processing. The list contains: the nature of the data, the purpose for which the data is intended, the duration of the intended processing, the general or specific data-protection provisions applying to the requesting authority, and whether or not the entity has agreed to specific conditions required by Europol concerning the data.

Concentrating on data exchange for the purpose of prevention, detection, investigation, or prosecution of criminal offences, the list of data protection principles will be identified here that should apply as a minimum list of parameters to consider when assessing a third state's level of data protection. The specific characteristics of criminal investigations should be taken into account here. Time is of the essence in criminal investigations, but the secret nature of an ongoing investigation should also be considered. In addition, the fair trial rights of Art. 6 ECHR and the presumption of innocence it provides in are reasons why personal data collected for the purpose of prevention, detection, investigation, or prosecution of criminal offences should only be processed (and transferred) for this purpose or a purpose that is compatible therewith. That is the purpose limitation principle. Known as one of the basic data protection principles introduced by the Data Protection Convention, the purpose limitation principle prohibits processing of data for a purpose that is not compatible to the purpose the data were originally collected for. This principle was also mentioned as the first of the so-called "content principles" identified by the art. 29 WP in the above-mentioned discussion document. This document makes an inventory of the elements to consider when assessing adequacy of a third state's level of data protection. Also the Europol list starts with the purpose for which data are intended. Europol only deals with data that are processed for the purpose of prevention, detection, investigation, or prosecution of the criminal offences within the scope of the Europol Decision.

Due to the significance of the purpose limitation principle for data exchange in criminal matters, the purpose limitation principle should be one of the minimum requirements to be fulfilled when assessing the adequacy of a third state's data protection framework.

Art. 5 of the Data Protection Convention also states that the quality of data should be guarded, i.e. data should be accurate, updated when necessary and adequate. Furthermore, data should not be excessive in relation to the purpose they are gathered for. This is the proportionality principle. Careless handling of data and improper safeguarding of the proportionality principle can have crucial repercussions for an individual involved in a criminal investigation either as suspect, witness, or victim.

Third states' authorities that have received personal data from a Member State possibly want to transfer these data to another third state. It could then concern a third state whose level of data protection has not been assessed yet. Because data from a Member State could then be introduced into a data protection framework that does not support the EU data protection principles, this onward transfer of data should be restricted in the case of criminal matters. In investigations or prosecutions of criminal offences that have links to several states, however, an onward transfer could become necessary. Nevertheless, an adequate level of data protection should also be provided by the receiving third state.

Finally, technical and organizational security measures should be in place in order to prevent tampering or loss of data. These measures may not be laid down in national law, yet the data controller in the third state should provide for a level of data security that is sufficient and appropriate for the risks that the processing of data presents.

The 29 WP lists two more principles: the transparency principle and rights of access, rectification and opposition. However, when exchanging data for the purpose of prevention, detection, investigation, or prosecution of criminal offences, these principles cannot be guaranteed in every case – in the interest of the criminal investigation. For this reason, they should not be part of the minimum data protection rules included in an adequacy assessment. This does not mean they are not important and in case they can be enforced, i.e. when there is no risk of corrupting the criminal investigation, they naturally should be complied with.

Enforcement and supervision are not part of the content principles but are listed under a separate heading by the 29 WP. Supervisory mechanisms should be installed in a third state in order to provide for the enforcement of adequate protection of data transferred from an EU Member State. The 29 WP rightfully stated that it is more efficient to define the objectives to be achieved by these mechanisms rather than requiring their mere presence. The independence of these authorities is a prerequisite.

These principles and mechanisms should be part of the minimum aspects included in an adequacy assessment of data transfers for the purpose of prevention, detection, investigation, or prosecution of criminal offences. Obviously, the authority making the assessment should be allowed to include more aspects of a data protection legal framework.

### *Deciding authority*

It is still not clear which authority should make the adequacy assessment and decide whether a data transfer to a third state can be organized or not. The relevant EU legal instruments on data protection allow adequacy assessments made by

the Member States as well as by the European Commission. Directive 95/46/EC mentions both options, while the Framework Decision on Data Protection in Criminal Matters only mentions the Member States. Both options have advantages and disadvantages. When the Commission makes the assessment, this means that one uniform decision is taken on a third states' level of data protection on which all Member States can rely. Nevertheless, decisions on adequacy made by the Commission could be influenced by wider political and economic concerns in relation to the third state concerned (Raab and Bennet, 1997). Although, it should be highlighted here that when negotiating the EU-US agreements, the EU Member States – represented by the EU presidency – also omitted assessing the adequacy of the US level of data protection. Most likely political and/or economic concerns were the background for this omission.

In the case of assessments of adequacy made by Member States, different conclusions could be the result. Due to the lack of uniform rules on how the evaluations are performed, it is possible that Member States apply diverging methods or include different elements of data protection legislation into the assessment. For example, one Member State may also include the practical application of data protection legislation in the assessment, while another may only rely on "law in the books." The Commission has confirmed this concern already in 2003 in its first report on the implementation of Directive 95/46/EC that provides for the adequacy requirement in its Arts. 25 and 26. This concern was recently confirmed by a study of the national legislations.

It should be stressed that Member States have implemented the EU legal instruments on data protection but can still differ to a considerable extent. As Member States will make an adequacy assessment starting from the point of view of their own data protection regime, this could lead to differences in their assessments (Raab and Bennet, 1997).

A solution to these issues could be to make the art. 29 WP the central authority that makes the adequacy assessments and takes the decision to transfer data to a third state or not in matters that fall within the scope of Directive 95/46/EC.

The 29 WP is independent and already has the task of advising the Commission on the adequacy of third states. If the 29 WP would be in charge of making a binding decision upon the adequacy of third states, there are fewer chances of economic or political interests at the national or Commission levels prevailing over data protection interests. Furthermore, it would help avert the fact that national data protection legislations differ, which causes national assessments of a third state's adequacy level to differ. Making assessments by the 29 WP binding decisions for all Member States would thus not require a change in its working procedure, although it would naturally increase the workload of the members. It

would necessitate an amendment to Directive 95/46/EC which established the 29 WP. Nonetheless, the Directive is being reviewed in 2011 and the disappearance of the former three pillars makes amendments to the data protection framework necessary. Therefore, it is an excellent opportunity to introduce this widened competence for the 29 WP could be done at the moment of this review.

#### **4. Future opportunities**

With the above explained concerns and questions regarding the adequacy requirement, the next question should be how this situation of uncertainty can be improved in future. Even though the European Commission already called for the simplification of the adequacy procedure in 2003 a genuine review of the rules has only been planned recently. The technological developments of the past decade and globalization as well as the age of Directive 95/46/EC itself and the recognition that the 2008 Framework Decision on Data Protection in Criminal Matters is an ineffective legal instrument, have all contributed to the Commission's plans for reviewing the current legal framework. Conferences, public consultations and scientific studies should lead to the presentation of proposals for new data protection legislation in 2011.

This review of EU legislation on data protection is in progress at the same time as the negotiations for a general data protection agreement between the EU and the US. Background for this is the transatlantic cooperation that has been intensified since the terrorist attacks of 2001 in the US. After separate agreements on mutual legal assistance, on transfers of passenger name record data and financial data, the European Council asked the Commission to propose a general agreement with the US on data protection and, where necessary, data sharing for law enforcement purposes. One of the main questions to be answered then is whether the principles laid down in this agreement would not only apply to future agreements covering data exchange but also to the existing ones. Especially with regard to the adequacy requirement, this could mean that existing agreements should be renegotiated.

#### **1. Review of the data protection legal framework**

The European Commission spared no effort in gaining opinions and preparing for the review of the EU data protection legal framework. In an elaborate communication called "a comprehensive approach on personal data protection in the EU", ambitious key objectives and points of view were given. Also the European Data Protection Supervisor published a detailed opinion on the Commission's communication after he was consulted by the Commission to do so. With regard to the adequacy requirement, the chapter "the global dimension of data protection"

contains improvements to be made concerning the adequacy procedure on the one hand and the use of the data protection principles known in the EU as benchmarks for third states' data protection on the other hand.

The review will not touch upon the existing data protection principles as these are still valid in spite of technological advancements (Korff, 2010). The existing principles refer to the principles laid down in Art. 5 of the Data Protection Convention and Art. 6 of Directive 95/46/EC and include the above-mentioned purpose limitation principle, the data retention principle – data can not be stored longer than is necessary for the purpose they have been collected for – and the principles guarding the quality of personal data. These principles have been formulated in a general manner which makes them valid still 30 years after the adoption of the Data Protection Convention.

With regard to the global dimension of data protection and the adequacy requirement, it is not the requirement as such that is questioned. The Commission has no plans to abolish the adequacy requirement and open data transfers to third states, even though the above described experiences with the US seem to predict something different. On the contrary, the practical difficulties in making an adequacy assessment that have been described above are issues that need to be solved. This is the perfect opportunity for the Commission to introduce a comprehensive package of rules governing the adequacy requirement, including clarification on which authority should make the assessment and a checklist of criteria to consider while making the assessment. The proposal by the Commission is expected in the summer of 2011.

## **2. The transatlantic cooperation in criminal matters**

To date, the agreements governing data exchange between the EU and the US were limited in scope. The 2002 Europol-US Agreement and the 2006 Eurojust-US Agreement only cover data exchanged by Europol, respectively Eurojust and within the scope of their respective objectives. Data Protection in criminal matters is only a small part of the 2003 EU-US Mutual Legal Assistance Agreement which covers also other means of mutual assistance such as video-conferencing and joint investigation teams. The 2007 EU-US Agreement on the exchange of passenger name records (2007 PNR Agreement) and the 2010 TFTP Agreement both are limited to a specific type of data. It was thus necessary to create a general agreement with the US in which the ground rules are laid down for exchanging personal data between EU Member States' authorities and US authorities for the purpose of prevention, detection, investigation, or prosecution of criminal offences. Due to the above discussed issues regarding the adequacy requirement in the agreements with the US, a crucial question should be answered when negoti-

ating such general data protection agreement. Will the principles to be laid down in such an agreement apply not only to future agreements covering data exchange but also to existing ones? In its negotiating directives, the European Commission certainly seems to be willing to retroactively apply the new agreement: *“existing EU or Member States personal data transfer and processing agreements with the US for the purpose of preventing, investigating, detecting or prosecuting, criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters after a transitional period of three years.”* This statement could have a considerably affect the adequacy procedure for the following reasons.

Data transfers between the EU and the US that are regulated by four of the mentioned agreements would be changed. This does not mean that the 2007 PNR Agreement is not affected but this Agreement is currently being renegotiated as well due to the fact that it was only provisionally applied since 2007. As explained in this contribution, it is precisely in preparing these four agreements that the EU, Europol, and Eurojust have not complied with the adequacy requirement (De Busser, 2010). Due to the 2008 Framework Decision on Data Protection in Criminal Matters which provides in an adequacy requirement for agreements with third states in this field, the future EU-US Agreement on data protection should not be concluded without making an adequacy assessment.

If a full assessment of the US level of data protection were made, it would have the following effects on the content of existing legal instruments. Regarding the Europol-US Supplemental Agreement and the 2010 EU-US TFTP Agreement, this would mean that the assumption of an adequate level of data protection would finally be backed up by a genuine adequacy assessment, followed by a decision on the US' adequacy regarding data transfers with the EU. With regard to the 2003 EU-US MLA Agreement and the 2006 Eurojust-US Agreement, it would mean that the prohibition of generic restrictions has lost its meaning. However, one should not triumph too soon as on October 26, 2010, the Ambassador of the US Mission to the EU, William E. Kennard, declared during a hearing on the future EU-US Agreement on data protection in the European Parliament that the US does not wish to renegotiate the existing agreements.

When reading the aforementioned negotiating directives, it seems that the Commission has already found a solution for this problem. The Commission states that it considers it a desirable step for the US to ratify the Council of Europe Data Protection Convention and its Additional Protocol. The Data Protection Convention lays down the basic principles of data protection that have been implemented by the EU Member States, and its Additional Protocol is the general legal basis for the adequacy procedure. This means that if the US would agree to accede to these two legal instruments, there would be no need for the entire discussion

surrounding the adequacy procedure, as the US would oblige itself to implement the same data protection principles in its system. An adequacy assessment would then no longer be necessary. This idea is neither desirable nor realistic.

The proposed accession of the US to these legal instruments is not desirable due to the fundamental differences between the US system of data protection and that of the EU. These differences are fundamental because they concern the basic principles such as purpose limitation and data retention. For example, data retention as it is included in the Data Protection Convention means that data should not be stored longer than is necessary for the purpose that they were stored for. In the US data protection regime, no such general data retention rule is laid down. On the contrary, separate acts contain provisions that restrict the retention of specific data, such as Video Privacy Act that allows storage of video tape rental or sale records for a maximum of one year unless a court order has been obtained (18 USC §2710(e)). Research has proven that data protection legislation in the US and the EU is divergent rather than similar (De Busser, 2009).

The proposed accession of the US to the Data Protection Convention and its Additional Protocol is furthermore unrealistic for two reasons. Firstly, it is questionable whether it is a realistic option to ask a state with a legal history that has not been characterized by detailed data protection rules to change its attitude as well as its legislation and adhere to a set of formerly unknown principles that would have to be implemented in national law. Secondly, the history of EU-US cooperation in criminal matters has demonstrated that it is also not reasonable to expect the US to embrace our umbrella data protection system. The US has shown that they want smooth and trouble-free data exchange by for example including the prohibition of generic restrictions in the 2003 EU-US MLA Agreement. Therefore, a complete transformation of the US data protection regime should not be a goal. Mutual cooperation and finding compromises in requiring additional safeguards from the US when processing personal data originating from the EU, is a more realistic option.

### 3. Conclusion

The requirement to assess a third state's level of data protection in order to safeguard the EU principles on data protection is clearly a prerequisite that is not without problems. There is no doubt about its importance in general and for data transfers for the purpose of prevention, detection, investigation, or prosecution of criminal offences in particular. Due to the fact that its importance is unmistakable, it is all the more surprising to see how many questions with regard to this adequacy requirement and the fulfillment thereof, have not been answered yet.

The European Commission should grasp the opportunity that it has at the present time with the review of the EU's data protection legal framework in full progress, to also answer the questions regarding the adequacy requirement. However, answering the questions regarding the content and the authority competent for making the adequacy assessment and taking the decision regarding a third state's level of data protection is not enough. It is clear that more work is needed in making the mandatory nature of the adequacy requirement clear and making the rules on how to go about in assessing a third state's data protection framework. Centralizing this competence with the members of the 29 WP who are already familiar with making these assessments in the field of Community activities, would solve most issues. It will not solve all issues as the risk that a third state exercises pressure from a political point of view to receive a positive adequacy decision, cannot be entirely excluded. In addition, the 29 WP as central authority deciding upon the adequacy assessment can also not avoid that third states amend their data protection legislation in such manner that they would no longer have an adequate level of data protection. This is an aspect where also the 29 WP has to rely on the goodwill of the third state to send a notification whenever an amendment is enacted to a relevant piece of legislation.

With regard to the transatlantic cooperation and the adequacy requirement, this is also a matter that should be decided upon now. With a new EU-US agreement on data protection in criminal matters on the negotiation table, the most main question is the effect of this new legal instrument on the existing agreements. If the new agreement will in fact be applied retroactively, this could create a better application of the adequacy requirement because the existing agreements that ignored it should then be renegotiated which could lead to better compliance with the adequacy requirement. The idea of making the US a party to the Data Protection Convention and its Additional Protocol should be dropped as it is not realistic due to the experiences with the US in the cooperation in criminal matters.

All eyes are now on the Commission that should present the review of the data protection legislation in the summer of 2011 as well as the Commission representatives who are negotiating the new EU-US agreement on data protection in criminal matters.



# **E-government adoption in the EU: theoretical and methodological challenges in the study of the digital divide**

---

---

**Georgia Foteinou**

---

---

## **1. Introduction**

“Information and Communication Technologies (ICT) play an essential role in supporting daily life in today’s digital society. [...] e-Inclusion aims to achieve that “no one is left behind” in enjoying the benefits of ICT. e-Inclusion means both inclusive ICT and the use of ICT to achieve wider inclusion objectives. It focuses on participation of all individuals and communities in all aspects of the information society. e-Inclusion policy, therefore, aims at reducing gaps in ICT usage and promoting the use of ICT to overcome exclusion, and improve economic performance, employment opportunities, quality of life, social participation and cohesion”

(European Commission 2010: the Digital Agenda for Europe)

Europe’s Digital Agenda makes clear that no citizen should be left behind in the Information Society and accordingly the EU has introduced policies and guidelines aiming at reducing the digital gaps within countries. ‘e-Inclusion’ is closely related to European policies on social inclusion, education and culture, regional development, innovation, industry and internal market (EC 2011). However, when looking closely at the EU level, two different kinds of digital divide are evident: one within countries and another between countries. This study focuses at the national level and presents a theoretical approach in the study of this phenomenon, while discussing the methodological challenges of empirical investigation. First, it makes an attempt to present the research problem in a comparative perspective, whereas the examination of the adoption rates of e-Government versus e-Commerce uncovers two important issues: first, the fact that the EU suffers not only from ‘digitally excluded’ but also from ‘digitally reluctant’ citizens and, second, that e-Government growth rates lag behind compared to those of e-Commerce, while they exhibit an ‘unexplained’ variation (both over-time and cross-national).

The term ‘digitally reluctant’ is used here to define the people who have the skills, the knowledge and the technical means to use e-services but they prefer not to, due to unspecified factors. This research problem is unveiled when measuring the growth rates of Internet use by the general population versus those of e-Government and e-Commerce adoption rates. What is observed then in the EU, is low and sometimes negative growth rates in e-Government, while e-Commerce

follows a linear growth. For example the adoption rates of e-Government services over the period 2005-2010 had a growth rate of 39.1% in the EU-27, while those of e-Commerce had an impressive 72.2% growth rate. One may well assume that this is because of the low quality of the offered e-Government services compared to e-Commerce services. However, this is only a simplistic view of e-Government adoption in the EU, as the research unveils that e-Government exhibits much higher fluctuation over time than e-Commerce and, in fact, in 2008 a drop was observed in many European countries (Eurostat, 2011). This downward tendency is present up to date in a number of EU member states. Thus, a number of citizens who were previously using e-Government services stop doing so after a specific time point. Hence, we are talking about another kind of digital gap – this in which people are self-excluded from a category of e-services – those provided by their governments. How this ‘digital gap’ varies across Europe and how it is explained? This study is focusing at the gap between potential versus real usage of e-services and discusses the theoretical and methodological problems related with the analysis of this phenomenon.

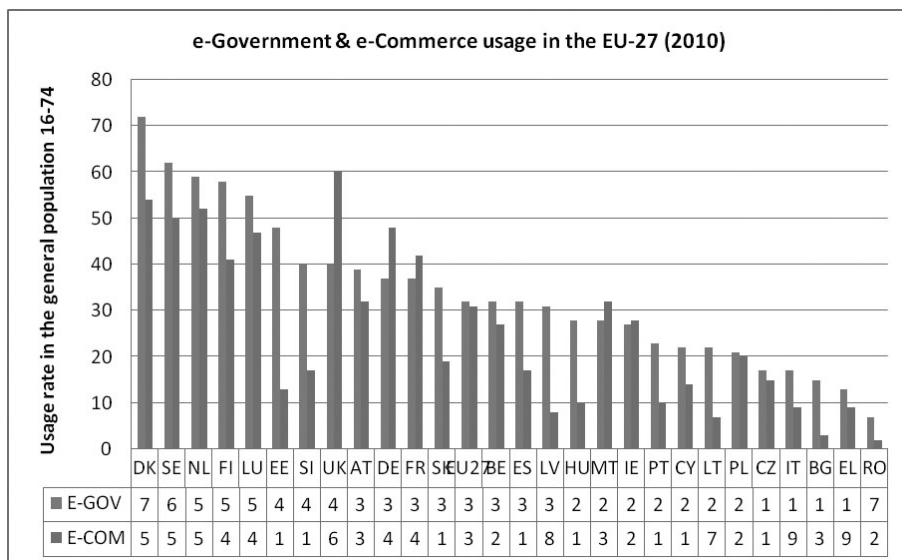
## **2. The ‘digitally reluctant’ Europeans**

An obvious answer to the question “why citizens do not use e-Government” could be that “because the offered services are not of high standards”. Yet, this applies to e-Commerce technologies and is not necessarily of equal importance in e-Government. Democratic principles and institutional factors have also been identified in literature as having a significant effect and thus a more comprehensive approach is needed. This does not imply that system quality and design issues do not matter, but rather that some more factors have an impact on the actual e-Government use. Thus, a question could be “why in a country, such the United Kingdom, with e-Government spending more the 1% of the GDP e-Commerce usage is about double than this of e-Government?” (UN, 2003). Are e-Commerce services so superior? And if yes, then it is the case only in the UK? To answer these questions we need to compare the e-Government usage rates with those of e-Commerce and also to take into account the general level of Internet use in the population.

In order to present more clearly the research problem we perform one comparative analysis and one longitudinal: comparing e-Government to e-Commerce, then comparing those levels in different countries and finally analyzing the over-time variation. This may give us some insights on the possible factors that may account for the observed variation across the EU. The following figure shows a

comparative view of the levels of e-Government and e-Commerce usage in the EU in 2010.<sup>1</sup>

**Figure 1.** E-Government and e-Commerce usage in the EU-27 in the general population 16-74 (2010)



Source: Eurostat 2011

At a first glance it is evident that the upper part of the graph is dominated by the Nordic countries along with Estonia, Luxembourg, Netherlands and Slovenia. The middle part is consisted of mainly Western European countries<sup>2</sup> (Germany, UK, France, Spain, Austria), while at the bottom we find mostly Eastern European and Mediterranean countries. Also, it unveils three very important 'outliers': UK, Germany and France. These three countries (along with Malta and Ireland) are the only ones where e-Commerce has, today, higher adoption rates than e-Government. In any other EU country the image is inverted, with e-Government having higher adoption levels. Another interesting characteristic of the three outliers is that they exhibit high over time variation with fluctuating usage rates.

1. Data available online at: [http://epp.eurostat.ec.europa.eu/portal/page/portal/product\\_details/dataset?p\\_product\\_code=TSDGO330](http://epp.eurostat.ec.europa.eu/portal/page/portal/product_details/dataset?p_product_code=TSDGO330) [http://epp.eurostat.ec.europa.eu/portal/page/portal/product\\_details/dataset?p\\_product\\_code=ISOC\\_EC\\_IBUY](http://epp.eurostat.ec.europa.eu/portal/page/portal/product_details/dataset?p_product_code=ISOC_EC_IBUY) and [http://epp.eurostat.ec.europa.eu/portal/page/portal/information\\_society/data/main\\_tables](http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/main_tables).

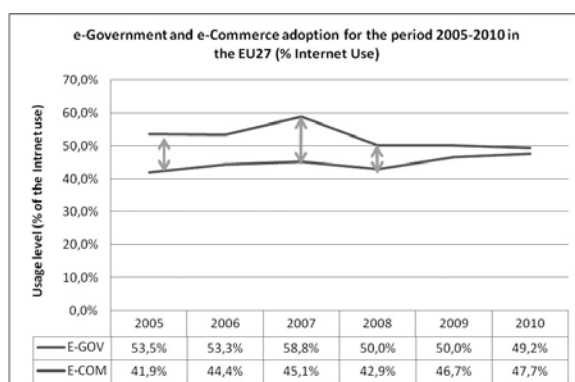
2. The term 'Western' does not denote solely the geographical position but also the cultural and economic background. For this reason Austria is classified as Western European although is not located in the West.

A longitudinal analysis of the usage levels of e-Government and e-Commerce in Europe shows that the two technologies follow different trajectories with e-Government exhibiting shifting adoption rates. In more detail, e-Government usage when measured as a percentage of Internet usage exhibits a downward tendency. More specifically, e-Government exhibits a decline of - 4.3 percentage points in the general population of internet users in a six-year period, while e-Commerce rises by +5.8 perc. points over the same period (2005-2010).

However, a more detailed analysis shows that different European countries have different adoption patterns while the above decline is observed only in a number of countries. Therefore, the dynamic nature of e-Government requires a different approach that is not static and presents e-Government acceptance by the general population as an on-going process. The absence of longitudinal and comparative studies in the EU however shows that mapping, first of all, the progress in Europe is imperative in order to understand the evolution of the phenomenon. Thus, a main challenge in the study of e-Government adoption levels is that the observed fluctuation cannot be described with any of the existing research models as they do not take into account over-time variation while they focus almost exclusively at the individual level. As such, they only have quite limited analytical value when it comes to longitudinal, trans-national studies.

The following graph shows that e-Commerce, when controlling for Internet connectivity, has an almost linear growth over time while e-Government usage rates exhibit greater fluctuation. To explain this decline, we cannot suppose that the quality of the services declines or that there are less services offered over time. Instead, a factor (or more) that may also fluctuate over time can account for the observed variation.

**Figure 2.** e-Government and e-Commerce usage growth in the EU-27 (2005-2010)



Source: Eurostat 2011

The above summary of the adoption rates shows that e-Government usage (as a percentage of the Internet usage) in the EU-27 has a downward tendency. In more detail, e-Government users in 2010 are only a 49.2% of the total of Internet users, while in 2005 was 53.5%. The most significant drop was observed in 2008, where in Germany the usage levels of e-Government dropped by 23% (from 43% in 2007 to 33% in 2008 following a drop of about 10 percentage units) and the United Kingdom where a drop of 16% was observed (from 38% in 2007 to 32% in 2008) (Eurostat, 2011).

This trend has been generally overlooked by the existing literature while none of the existing research models can describe such trend. From the proposed factors in e-Government adoption literature only trust in Government may exhibit such over-time fluctuation that may slow down e-Government adoption. However, this explanation is also dubious as, although some empirical studies support this explanation, some others disprove it. Hence, the primary research problem when trying to identifying the possible causes of such fluctuation is to build a research model which can describe and predict such over-time variation.

In short, this study aims at identifying the research challenges when analyzing the gap between different technologies in the EU. The most widely used approach for this kind of research questions is to utilize e-Commerce theories and methodologies to analyze e-Government. It seems, however, that the two technologies are not influenced by the same factors, and thus the utilization of e-Commerce research models to explain e-Government is a sub-optimal (if not incorrect) research methodology. Nonetheless, in practice, most empirical e-Government studies use research models developed in e-Commerce literature. By doing so, they fail to take into account the additional factors which produce the observed differences between the two technologies.

### **3. What influences e-Government adoption?**

E-Government acceptance factors have become the object of various studies as the literature is slowly moving from the supply-side to the demand-side. Thus, while at its early years e-Government research was more focused on availability issues, systems architecture, software development and infrastructure, it turns now to less technical issues and it focuses more on the final technology recipients and their needs. Also, the over-optimism that initially surrounded e-Government has been now put under question and this leads to a need to re-define the purpose and the expectations from technology – this time including also citizens in the debate. Why citizens use or do not use e-Government services? What affects their intention to engage or not in e-Government? Why are they often reluctant

and what are the underlying factors behind this attitude? Is it all purely a matter of design or there are more fundamental reasons for such scepticism?

Some parts of these questions have been answered, while some others remain still unanswered. A number of factors have been identified in the literature that leads to one or another explanation. However, none of the existing explanations provides definite answers as the empirical investigation produces mixed and sometimes contradictory results. In general, the existing explanatory variables are summarised in service quality, Internet access, environment of innovation, privacy concerns, risk perceptions and trust. In some exceptional cases other explanations have also been given. These include the regulatory framework, cultural characteristics and number of offered services. Nonetheless, there are cases where most of the above conditions are satisfied but e-Government acceptance levels remain surprisingly low - even for the e-Government forerunners. Why do the usage levels of the on-line tax filling and payments systems in the United States and Taiwan - two of the most advanced countries in e-Government technology - remain as low as 20% - 22% of the total of tax-payers the last few years? (Hung et al. 2006). Why, some advanced European countries such as the United Kingdom and Germany exhibit similar adoption patterns with high levels of digitally 'reluctant' citizens?

It is evident that some factors remain unexplored or under-explored and a part is missing from the research puzzle to connect the seemingly unrelated aspects of the question. Utilising static, individual level, research models to explain dynamic longitudinal phenomena can lead to inconclusive results. Individuals do not only have 'rational' motives as they are often influenced in their decisions by the cultural and institutional environment in which they live. Hence, research in e-Government acceptance cannot be complete without taking into account the broader political and institutional environment in which technology is developed and diffused.

The following section gathers together the different approaches in literature and examines some of the most possible explanations. The criteria according to which the reviewed studies have been classified are, first, the theoretical approach and the explanatory variables used to predict or explain e-Government adoption and second the empirical investigation of the phenomenon. There is a growing body of literature suggesting that Trust of the Internet (TOI) and Trust of the Government (TOG) has a decisive role in e-Government acceptance. Nonetheless, some studies disprove this hypothesis and this makes the trust hypothesis dubious. For this reason, special attention is paid at the trust literature, while at the final section of paper an alternative theoretical approach is discussed.

#### **4. Theoretical approaches and empirical studies of e-Government adoption**

E-Government diffusion and adoption has become the subject of various studies which aim to explore and specify the factors which contribute to successful e-Government adoption by citizens. Among them, there are some studies which focus, not only to the traditional technology adoption factors, but also to the factors behind the “digitally reluctant” citizens. Digitally reluctant are those citizens who have the material resources and the knowledge to use ICT but they choose not to due to a lack of motivation, confidence and/or trust (Codagnone & Osimo, 2009). This category of self-excluded citizens seems to be the key for explaining the differences between countries which are technologically advanced but e-Government usage remains relatively low (or lower than the expected levels).

The first finding of the literature review is that there is an incomplete definition of e-Government adoption. In most studies it is not clear if the term e-Government “adoption” refers to the citizens who repeatedly use e-services, to the citizens who are willing to use e-services or to the citizens who occasionally use e-services. Such distinction between the individual characteristics which raise a higher probability of adopting e-Government and the behavioural intention to use e-Government is necessary in order to classify the existing approaches to the question. So, depending on the ‘lenses’ through which technology is viewed, some studies may focus on:

- (a) the characteristics of the citizens who are already users (Reddick, 2005; West, 2004; Akman et al. 2005; Foteinou, 2010) or
- (b) the availability of e-services and the service characteristics which increase users’ satisfaction (Barnes & Vidgen, 2006; Choundrie et al., 2005; Gilbert & Balistrini, 2004), or
- (c) the initial intention to use e-Government services (Carter & Belanger, 2008; Warkentin et al. 2002; Horst et al., 2007).

Therefore, some studies focus on more technical aspects such as digital infrastructure or quality/availability of services, while others focus on the citizens’ subjective norms and perceptions which affect the intention to use e-services.

A second finding of the literature review is that most empirical studies focus on the individual level and tend to underestimate environmental factors. However, people in different countries adopt technology in different ways and for different reasons related to their subjective perceptions and norms. Trying to identify patterns of adoption non-related to a specific cultural and institutional environment poses serious challenges, especially in view of the lack of transnational and longi-

tudinal studies. Moreover, analysing e-Government as a value-neutral technology that does not affect and is not affected by the environment in which is developed and deployed creates questions about the epistemological perspective which is adopted. Apart from a few studies which clearly mention that a rational actors approach is adopted, the rest do not specify how technology is viewed in their analysis. Another characteristic of e-Government research is that most of the empirical studies use models and methodologies drawn from e-Commerce literature and they analyse e-Government as if they had exactly the same determinants.

However, Jane Fountain (2001) argues that studies that focus on the individual level are inconclusive and contradictory and they compare different and non-comparable technologies as if they were similar (Fountain, 2001: p. 89). As a result, most of the existing studies focus on technology in isolation without assessing environmental factors or the vast differences in governments & Bailur, 2007). Subsequently, research captures only some aspects of the problem, following quite often a data-driven approach. However, individual level studies alone cannot offer generalizable results as they quite often ignore the broader picture, while the lack of theories specific to e-Government contributes a lot to this partial consideration of the research problem. In contrast, this paper compares critically the adoption levels of both e-Government and e-Commerce aiming at showing that these two technologies do not have the same determinants and thus a different approach is required.

## 5. Theoretical approaches

Two approaches are predominant in e-Government adoption literature: the first is based on the Technology Acceptance Model (TAM) and the second refers to the on-line trust literature while some studies use a combination of the two (Carter, 2008). There are also studies which adopt different theoretical models either in combination with the aforementioned models or by utilising completely different research approaches. The most frequently cited are the theory of reasoned action (TRA), the Diffusion of Innovation theory (DOI), the motivational model and the theory of planned behaviour (Carter, 2010). With the only exception of Diffusion of Innovation theory, all the other approaches adopt a rational actors perspective and they analyse technology acceptance exclusively at the individual level.

Nonetheless, there are some studies which examine e-Government adoption at the national level by utilising the aforementioned models or by using descriptive and exploratory research methodologies. However, utilising individual-level variables to explain country-level phenomena can be quite misleading as they ignore the broader image and the national differences. At this point, it is useful to classify the theoretical models in rational actors approaches and institutional or



other approaches. In the following tables the main theoretical approaches and the most cited empirical studies in each category are presented.

**Table 1.** Main Theoretical Approaches in e-Government Adoption Literature

Theoretical framework	Studies Based on the Framework	Explanatory variables
Technology Acceptance Model (TAM)	Davis (1989), Carter & Belanger (2005 & 2008), Dimitrova & Chen (2006), Gilbert et al. (2004), Horst et al. (2007), Warkentin et al. (2001), Wang (2003), Wu & Chen (2005)	Perceived Usefulness (PU), Perceived Ease of Use (PEOU), Previous Positive Experience, Perceived Credibility
Computer self-Efficacy	AlAwadhi & Morris (2008), Warkentin et al. (2001), Wangpipatwong et al. (2008)	Computer self-efficacy, TOG, PU, PEOU, Perceived Risk, Cultural Characteristics which affect Uncertainty avoidance, effective interaction over the net
Theory of Planned Behaviour	Warkentin et al. (2002), Horst et al. (2007), Hung et al. (2006), Kanat & Özkan (2009), Gilbert and Balestrini (2004), Wu & Chen (2005)	Risk & Uncertainty Avoidance, PU, PEOU, effective interaction over the net
Trust literature	Carter & Belanger (2005), Belanger & Carter (2008), Reddick (2005), West (2004), Riedl (2004), Warkentin et al. (2002)	Trust of the actor providing the service, General Predisposition to trust, Social Demographics (gender, education etc.), Party Affiliation, Cultural factors, Risk perceptions
Diffusion of Innovation Theory	Roger (1983), Fu et al. (2006), Schaupp & Carter (2005), Carter & Belanger (2005)	Time, Environment of Innovation
Motivational Model	Kumar et al (2007)	User Characteristics, Satisfaction, Web-site Design, Perceived Control over the process, Perceived Usefulness, User Expectations
Data-driven studies	Bavec & Vintar (2006), Boyer-Wright & Kottemann (2008),	Economic Development, Innovation, Internet Connectivity, National Performance Indicators

The literature review shows that too few studies use approaches other than those of rational actors perspectives. The few studies that examine e-Government acceptance at the national level are mostly data-driven and thus they lack a strong causal explanation.

It is common ground in e-Government literature that the lack of well-developed theories makes the analysis of acceptance or the impact of e-Government quite

problematic as it usually leads in low-quality and often ungrounded generalisations (Heeks and Bailure, 2007). From the proposed theoretical approaches in e-Government literature, neo-institutionalism seems to be the most promising as it may capture the impact of institutional factors and path-dependencies very well (Fountain 2001; Yang 2003; Heeks & Bailur, 2007; Yildiz (2007)). The following section examines an institutional approach to e-Government acceptance which puts the trust literature in a broader theoretical framework of technology acceptance.

## **6. An institutional approach in e-Government adoption**

### ***6.1 Defining e-Government acceptance and adoption***

Most of the previous e-Government adoption studies do not clearly define what is adoption. Two of the most influential authors in e-Government adoption, Carter and Belanger (2005) associate adoption with the intent to use, while Warkentin et al. (2002) consider acceptance as the initial intention of the citizens to engage to e-Government regardless of the purpose of use. Also, Gilbert and Balestrini (2004), measure it as intention to engage to e-Government. Thus, it seems that adoption is associated with the intention to use. However, it seems that, in general, the existing studies do not take into account the purpose of e-Government use (to obtain information, to download forms, to make on-line transactions etc.). Yet, e-Government adoption is a multidimensional concept as not only the purpose but also the frequency has a role; using a service once a year is not the same as frequent use. Therefore, how 'loyal' the users are and how far they are willing to go may lead to a different definition of acceptance. If, for example, the use of e-Government is legally binding has also a role in defining 'acceptance'.

Another question when defining adoption is the e-Government stage. Reddick (2005) distinguish two phases in e-Government adoption: The first is the information dissemination phase where the citizens use e-Government systems to obtain information about services, political issues etc. while the second is the transaction-based e-Government. According to Reddick, both phases are closely intertwined with the street level bureaucracy and he examines trust as an important element of e-Government adoption.

### ***6.2 Re-conceptualizing and operationalizing an under-specified term: Trust in Government***

The literature review shows that researchers define trust in many different ways and this creates measurement problems; not all models measure the same thing or refer to the same thing. Thus, 'What is trust?' is a rather important question in any research that aspires to clarify the role of trust in e-Government acceptance. However, most authors – if not all – do not adopt a definition of the term drawn

from political science and instead they use general definitions drawn from sociology or psychology that mostly refer to interpersonal trust. This paper adopts an institutional perspective on the role of trust and thus it utilises trust as an endogenous factor which is influenced by institutional performance.

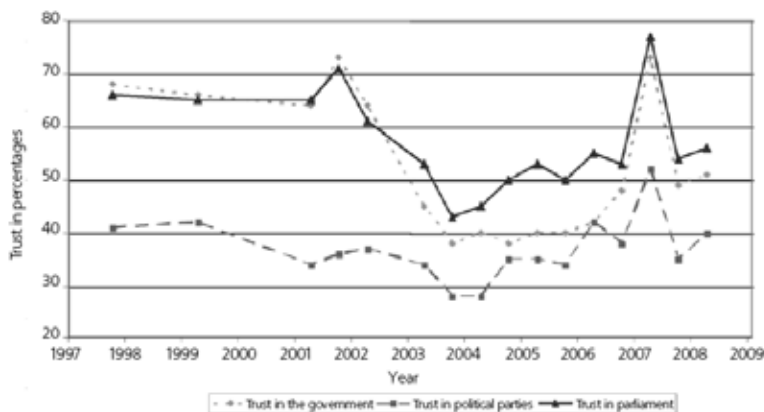
However, in order to define trust of the government (TOG) we need to define, first, what government is – or, better yet, what citizens think government is – and what the meaning of ‘trust’ is for citizens. When examining citizens’ responses to the question ‘What is government?’ are likely to vary considerably; they may answer the governing political party, the public administration, the health system, the city council, the state government etc. The concept of trust has also many implications, as trust implies a level of uncertainty; but, uncertainty about what? Not all people across Europe face the same risks. Actually, citizens in different countries face different uncertainties and thus they have different expectations from their governments. So, in some countries trust in government may depend on a lack of corruption, or may be perceived as satisfaction with democracy, competence of the government, efficiency and so on. Hence, trust does not have the same meaning for all Europeans and it actually depends on the different expectations citizens have from their governments. Therefore, trust does not solely depend on the actual performance or responsiveness of the government but also on the citizens’ expectations and, thus, it inevitably entails a degree of subjectivity that need to be dealt with.

### ***6.3 Operationalisation of the term***

Christensen and Laegreid (2003) showed that trust does not necessarily depend on citizens’ practical experiences with any specific administrative units, but instead that their trust in government is of a general nature. In fact, there is a strong correlation between trust in the different institutions as high levels of trust in one institution correlate with high levels of trust in other institutions. The authors acknowledge the fact that trust is a multi-dimensional concept and there is no one-factor explanation for the variation of citizens’ trust in government. They conclude, however, that the best predictor of citizens’ trust in government is the regime’s performance and the level of satisfaction towards democracy. This is in accordance with the research findings by Mishler and Rose (2001) who empirically examined institutional trust in Central and Eastern Europe exploring several dimensions of trust including trust in the parliament, the courts, the police etc. The authors conclude that in this group of countries perceptions of factors such as economic performance and corruption have a significant impact. In contrast they found that socio-economic variables are not good predictors of trust.

Another research study in the Netherlands by Hendriks (2009) confirms these research results, as the correlation between the levels of trust in different institutions is evident. Figure 3 shows Hendriks’ findings.

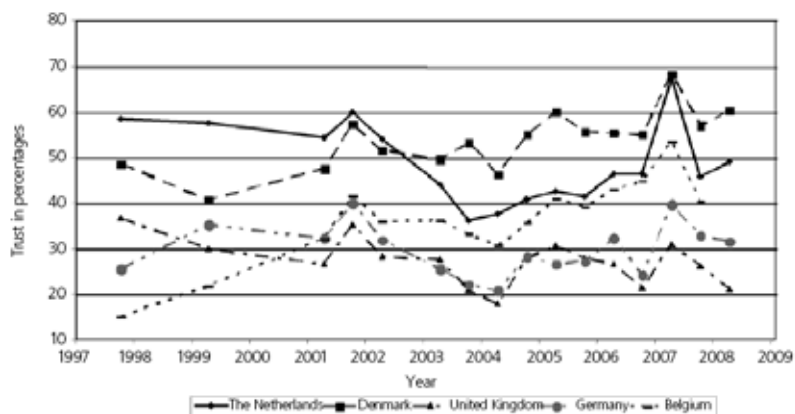
**Figure 3.** Trust in different political Institutions in the Netherlands  
(Results by Hendriks, 2009)



Source: Eurobarometer 2010

Moreover, this research demonstrates co-variance of the levels of trust between European countries and the general trends around Europe. As such, among a number of possible approaches to trust, a macro-performance approach is the most appropriate as it seems that Europeans are strongly influenced by common factors (see Figure 3) and it can also best explain the synchronous fluctuation in a number of different countries.

**Figure 4.** Trust in political institutions in five European countries  
(Hendriks, 2009) Source: Eurobarometer



The macro-performance approach leaves aside the individuals' risk perceptions and instead focuses on the governments' performance and the level of satisfaction with democracy. It is based on the idea that citizens have clear expectations and there is a general consensus of what tasks should be performed by their government. It refers to the issues that are considered as important (and not as secondary tasks of the government) by the majority of the population; for example, economic growth, social security, unemployment etc. (Bouckaert et al., 2002; Citrin & Green, 1996). It also takes into account previous experiences with public administration that lead citizens to form opinions about the performance and responsiveness of their governments. The trust variable has been repeatedly measured in Standard Eurobarometers through the question: "I would like to ask you a question about how much trust you have in the (NATIONALITY) Government? Please tell me if you tend to trust it or tend not to trust it."

#### ***6.4 Theoretical Lenses: a Neo-Institutional Approach***

In recent years, there has been an increasing interest on how technology can transform government or how technology may influence political regimes. On the other hand, there is the view that technology in the public sector is only the means to an end and not a driving force for change. However, the view of technology as an objective, external force, overlooks the role of human actors and implies that technology will inevitably improve the way a government operates. At the same time, there is a large volume of recent studies emphasising the social characteristics of technology and how social structures shape technology through strategic choice and social action. Quite often, e-Government literature seems divided between technological determinism and social constructivism. Between the two extremes, however, there are many approaches which manage to reconcile these two different views of technology. This paper supports the view that technology and institutional and political structures are not independent and their interaction affects the technology adoption patterns. Therefore, in this study a neo-institutional perspective is adopted. Although there are no complete theories in e-Government, Fountain's (2001) Technology Enactment Framework and Orlikowsky's (2000) Structural Model of Technology can contribute much in our understanding of e-Government adoption in specific institutional environments.

The review of the literature shows that technical, economic and cultural factors are not enough to explain e-Government adoption and thus the assumption that technology and institutions interact is quite strong. However, there is no coherent theoretical framework to produce testable hypotheses and thus most studies utilise research models borrowed from e-Commerce literature. However, utilising the same or similar research models to explain phenomena which follow different trajectories is not a correct research strategy. This paper adopts the view

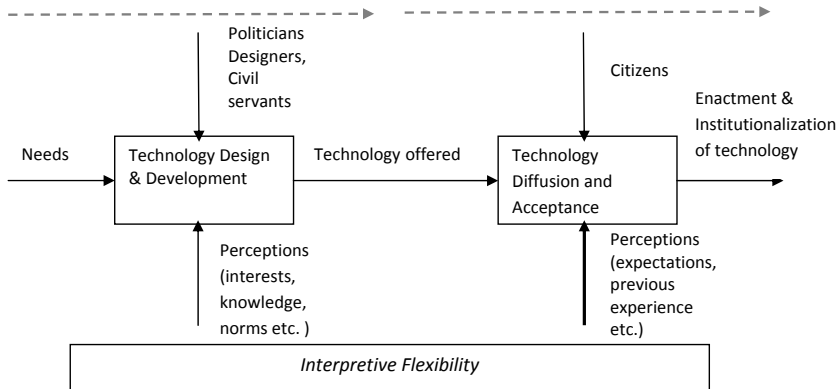
that perceiving e-Government technologies as both social and physical artefacts is quite useful in explaining how technology and institutions affect each other in various ways. Both theoretical approaches put emphasis in the dual nature of technology while they stress the separation of embedded and objective technology. Technology is physical and objective in the sense that is designed to meet engineering requirements and to reflect assumptions on how technology should be applied in the everyday business of public administration. Synchronously, technology is social in the sense that has embedded rules and structures which reflect norms of the institutional and social environment in which its use is nested. Thus, technology is not objective – although it has objective characteristics – and it can be viewed differently from different actors.

Orlikowsky (2000) at the Structurational Model of Technology identifies two stages in technology development and adoption: the first is where politicians, designers, civil servants etc. design and develop technology according to their knowledge, interests and norms, while the second is where users enact technology if it is in accordance with their perceptions and interests. Technology has some objective characteristics (functionality, response times, capacity etc.) but each of these groups of actors perceive technology in subjective ways. If these actors repeatedly use technology in the way technology has been designed to be used, then this technology is 'routinised' and becomes part of the everyday way of interacting. If this process lasts for long, then technology starts affecting social structures because it gradually becomes part of the structure and thus it is difficult not to comply with these technology-mediated processes; it is institutionalised. In this last stage, if successful, we can start talking about a 'soft' type of technological determinism; technology then 'embodies' structures which (re)present various social rules and political interests and starts affecting the social structure in which its use is embedded.

However, things are not so evident because of the flexibility of the perceptions about technology. The same system can be understood and used by different actors in vastly different ways. This is the way of the 'users' to affect technology and to agree or disagree with the interests, purposes and institutional context which is embodied in technology. After a trial period, technology will be adopted, redesigned, abandoned or replaced following a technology life-cycle. Depending on the level of acceptance, technology will gradually be legitimised and institutionalised. However, things become more complicated if we look at different systems. Two e-Government systems may have exactly the same functionality – for example, they may be designed to facilitate an electronic tax declaration – but there is a plethora of ways to design such system (even if the final output is exactly the same). The design of an e-Government system may take a number of different forms, not only because engineers have different views, but also because the legislation and norms which are embedded in each system differ in different

countries. When individuals use the system, then, they unconsciously and repeatedly enact a set of rules and norms that are embedded in the specific system. From this point of view, the role of users is crucial as “structures are not located in organizations or in technology, but are enacted by users”. Figure 4 shows how technology is adopted and institutionalised according to Orlikowsky:

**Figure 5. The Structural Model of Technology**



But what are the determining factors behind e-Government acceptance? Fountain (2001) gives us some theoretical insights when she states that individuals are inclined to enact new technology: “to reproduce existing rules, routines, norms, and power relations if institutional rules are clear and no salient alternative uses are visible in the environment”. Therefore, in addition to the ‘traditional’ technology adoption factors (i.e. usability issues, infrastructure), Fountain explains that in e-Government institutional variables have also a role and she focuses at the norms and rules which are embedded in technology. This implies that when individuals do not trust the specific institutional context in which technology is embedded then they do not ‘enact’ technology by not using it. They avoid in this way the institutionalization of technology, and thus the subsequent acceptance of the rules and control mechanisms which are embodied in it. This process, although not conscious most times, offers some understanding of why trust in government may have a decisive role in e-Government adoption.

Castells (1996), however, in his seminal work, argues that the impact of e-Government stretches far beyond the limited scope of public administration and public policy as technological developments lead in new forms of political interaction. The EU has set relevant policies and guidelines to address the issues arising from the adoption of ICT’s in the public sector and to ensure elimination of digital divides. The goal is to address the challenges of developing sufficient ICT infrastructure, services and skills while stimulating the economy and preventing

digital exclusion of citizens. However, in some countries a paradoxical phenomenon occurs where intense focus on government service delivery widens the gap between citizens and public administration. Fountain (2001) argues that this happens because governments are involved in complex political processes and cannot be seen by the citizens only as agents offering services. Defining the governments as production companies and treating citizens as consumers ignore the inherent political character of the public sector and eventually leads to greater scepticism by the citizens. According to Fountain, by overlooking the notions of good governance and citizenship and focusing only on service delivery may lead in growing distrust instead of building trust.

## 7. Conclusions

This paper stresses the inherent weaknesses of the existing e-Government research methodologies in the study of e-Government adoption. What this paper shows is that when examining the over-time variation of e-Government usage levels we observe an unexplained variation across Europe. This variation cannot be described by the existing research models as the focus on the individual level takes only a snap-shot of e-Government usage and ignores the dynamic nature of technology adoption. Thus, the existing 'static' research models fail to take into account the macro-level factors which affect adoption and they lead in inconclusive research findings.

This study explores an alternative theoretical approach based on institutional theory that can offer some theoretical insights on the reasons which lead on growing scepticism on the part of citizens. Institutionalism has been supported by many authors as the most promising theoretical approach in e-Government research. However, the inability to extract testable hypotheses has discouraged many researchers from utilising institutionalism in empirical research. This paper shows that an institutional approach is consistent with the pre-dominant trust literature but offers the additional advantage of exploring e-Government adoption within an institutional framework, instead of exploring trust as a single factor. The only modification needed is to re-define trust not as interpersonal trust but as institutional trust that is more relevant to political phenomena. This definition of trust, unlike the existing approaches, measures trust not in specific public agents offering services, but in the government as a whole. Thus, it identifies government not as agents offering services but as political entities that form people's views and perceptions.



## References

- Akman I., Yazici A., & Arifoglu A. (2005), 'e-Government: a global view and an empirical evaluation of some attributes of citizens', *Government Information Quarterly*, vol. 22, pp. 239-257.
- AlAwadh S. & Morris A. (2008), 'The Use of the UTAUT Model in the Adoption of E-government Services in Kuwait', *Proceedings of the 41st Hawaii International Conference on System Sciences*, pp. 1-11.
- Barnes J. & Vidgen T. (2006) 'Data triangulation and web quality metrics: a case study in e-Government', *Information and Management*, vol. 43, pp. 767-777.
- Bavec C. & Vintar M. (2007), 'What Matters in the Development of the E-Government in the EU?', *Lecture Notes in Computer Science*, vol. 4656/2007, pp. 424-435.
- Bouckaert G., Van de Walle S., Maddens B. and Kampen J. (2002), '*Identity vs performance: an overview of theories explaining trust in government*' in *Quality and Trust in Government*. Leuven, Belgium: Public Management Instituut voor de Overheid, Katholieke Universiteit Leuven.
- Carter L. (2008), 'E-government diffusion: a comparison of adoption constructs', *Transforming Government: People, Process and Policy*, vol. 2 (3), pp. 147-161.
- Castells M. (1996), *The rise of the network society*, Malden, MA: Blackwell.
- Choundrie J., Weerakkody V. & Jones S. (2005) 'Realising e-Government in the UK: Rural and Urban Challenges', *Journal of Enterprise Information Management*, vol. 18(5), pp. 568-585.
- Citrin, J. and Green D.P. (1996), 'Presidential Leadership and the Resurgence of Trust in Government', *British Journal of Political Science*, Vol. 16(4), pp. 431-453.
- Codagnone C. & Osimo D. (2009), 'E-government current challenges and future scenarios', in Nixon P., Koutrakou V. & Rawal R. (eds) *Understanding e-Government in Europe*, Routledge, New York.
- Foteinou G. (2010), 'e-Exclusion and the Gender Digital Divide', *ACM SIGCAS, Computers and Society*, Vol. 40(3), pp. 50 -61.
- Fountain J. (2001), *Building the Virtual State: Information Technology and Institutional Change*, Brookings Institution Press, Washington, D.C.
- Fu R. Farm K. & Chao P. (2006), 'Acceptance of electronic tax filling: a study of taxpayer intentions', *Information and Management*, vol. 43, pp. 109-126.

Gilbert D., Balestrini P. (2004), 'Barriers and Benefits in the adoption of e-Government', *International Journal of Public Sector Management*, vol. 17(4), pp. 286-301.

Heeks R. & Bailur S. (2007), 'Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice', *Government Information Quarterly*, vol. 24, pp. 243-265.

Hendriks F. (2009), 'Contextualizing the Dutch drop in political trust: connecting underlying factors', *International Review of Administrative Sciences*, Vol. 75(3), pp. 473-492.

Horst M., Kuttschreuter M., & Guttelin J. (2007), 'Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands', *Computers in Human Behavior*, vol. 23, pp. 1838-185.

Hung S., Chang C., Ting-Jing & Yu T. (2006), 'Determinants of user acceptance of the e-Government services: The case of online tax filing and payment system', *Government Information Quarterly*, vol. 23, pp. 97 - 122.

Kanat I. & Ozgan S. (2009), 'Explaining Citizen Adoption of Government to Citizen Services: A Model Based on Theory of Planned Behaviour (TPB)', *European and Mediterranean Conference on Information Systems 2009*, July 13-14, Izmir, Turkey.

Kumar V., Mukerji B, Butt I. and Persaud A. (2007) 'Factors for Successful e-Government Adoption: a Conceptual Framework', *The Electronic Journal of e-Government*, vol. 5(1), pp. 63 - 76.

Mishler W. & Rose R. (2001), 'What are the Origins of Political Trust? Testing Institutional and Cultural Theories in Post Communist Societies', *Comparative Political Studies*, vol. 34, pp. 30-62.

Moon J. & Norris D. (2005), 'Does managerial orientation matters? The adoption of reinventing government and e-Government at the municipal level', *Information Systems Journal*, vol. 15, pp. 43-60.

Orlikowski W. J. (2000). 'Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations', *Organization Science*, vol. 11(4), pp. 404-428.

Reddick C. (2005), 'Citizen interaction with e-government: from the streets to servers?', *Government Information Quarterly*, vol. 22, pp. 38-57.

Riedl R. (2004), 'Rethinking trust and confidence in European e-government: Linking the public sector with post-modern society' in W. Lamersdorf, V. Tscham-

mer, and S. Amarger (eds.), *Building the E-Service Society: E-Commerce, E-Business, and E-Government*. Norvell, MA: Kluwer, pp. 89-108.

Titah R. & Barki H. (2006), 'E-Government adoption and acceptance: A literature review', *International Journal of Electronic Government Research*, vol. 2(3), pp. 23-57.

Wang Y. (2003), 'The adoption of electronic tax filing systems: an empirical study', *Government Information Quarterly*, vol. 20(4), pp. 333-352.

Wangpipatwong, S. Chutimaskul, W. & Papasratorn, B. (2008) "Understanding Citizen's Continuance Intention to Use e-Government Website: a Composite View of Technology Acceptance Model and Computer Self-Efficacy", *The Electronic Journal of e-Government*, vol. 6(1), pp. 55-64.

Warkentin, M., Gefen D., Pavlou P. and Rose G. M.(2001) 'Encouraging Citizen Adoption of e-Government by Building Trust', *Electronic Markets*, vol. 12(3), pp. 157-16.

West D. (2004), 'E-government and the Transformation of Service Delivery and Citizen Attitudes', *Public Administration Review*, vol. 64, pp. 15-27.

# **Libraries and the role of copyright exceptions and limitations in the contemporary academic environment**

---

---

**Anna Fragkou & Vassiliki Strakantouna**

---

---

## **1. Introduction**

Libraries have always been the reservoirs of expressed knowledge, the curators of human intellectual creation, the channels to information and the gateways to disseminate all the above to the public. New technologies have transformed libraries not only in the way they organize information and provide access to it. Nowadays, libraries' collections include not only print material, but also digitized (i.e. formerly print) or electronically born material. New technologies and more specifically information technologies (IT) have changed not only their collections, but also the way libraries operate and serve their users. Today's libraries are digital, virtual and with no physical borders as they offer their services online without the need for the user to physically visit the libraries' premises. According to Ridley [Ridley, 2005], "new technologies, IT and digital libraries are not just tools to be learned and used. IT is an environment in which we operate and are immersed. IT is an ecology".

However developed, today's libraries still rely on traditional concepts and functions in order to serve their users. Namely, they have to:

- a. Acquire (either by purchase or through licensing) and organize their material effectively in order to facilitate the access to it.
- b. Make their material available to users through circulation and inter-library loan services, and more recently by providing remote online access to it.
- c. Preserve their material, i.e. documented intellectual creation, for the longest possible period of time.
- d. Customize their services to accommodate the current needs in information seeking and provision.

Almost all of the above library functions are related to and influenced by intellectual property legislation. In order to operate, libraries provide reproduction services to their users, loan their material for a certain period of time, co-operate with other libraries in resource sharing systems (inter-library loan), transform

their material for preservation or digital curation purposes and for facilitating access to it, and more recently, they are getting involved in producing their own -digital in most cases- material. Librarians and information professionals know that copyright compliance is both a legal and an ethical issue. In their activities, they need to ensure that they remain on the right side of the law and that their conduct is ethical (Pedley, 2007). The principles of respecting the user's right to access to information and, simultaneously, to preserve the creator's or copyright holder's rights, are described with clarity in many librarians codes of ethics (most of them are accessible via IFLA's website). These codes of ethics bind librarians to the users and constitute a means of self-regulation the potential conflicts between the freedom of access and the copyright protection to (Strakantouna, 2010).

Libraries, both in "traditional" and digital environments, in the process of material's management and the rendering of services often face many issues related to copyright that mainly concern two exclusive and absolute rights of the authors. The right of the exploitation of a work (property right) and the right to protect the author's personal bond with his/her work (moral right), which according to copyright (art 1. par. 1 of the Greek Copyright Law 2121/1993) are automatically granted to the authors. The right of the exploitation of a work for social cultural and educational policy reasons in all national legislations, international treaties and European Union Directives is subjected to exceptions/limitations that concern its content and its extent. Except the term «limitations», the term «exceptions» is often used either accumulatively or alternatively. The first one implies the unauthorized but paid use of a work, and the second the free use without remuneration. In spite of the difference in the various conceptual approaches, those two terms are synonymous and concern concrete legislative regulations on the extent and the content of the property right (Kallinikou, 2007).

Copyright exceptions and limitations are the tools that libraries are provided to use in order to continue providing their services, supporting innovation, creativity and economic growth in all parts of the world. However, how easy it is for today's libraries to comply with copyright rules which seem to get stricter and via stricter new copyright, or copyright-related, trans-national conventions, powerful trade agreements that address the use of copyrighted products, tightly binding access licenses, and sophisticated digital rights management (DRM) tools that restrict access to resources and prevent circumvention of digital material, even if they are purposed to facilitate preservation activities or to provide access to people with disabilities?

In the 21st century there is a great necessity to re-examine copyright as well as an immediate need for corresponding action among all the interested parties worldwide. Exceptions/limitations and other public interest, considerations should be more explicitly addressed within the global framework and should be viewed as public rights that balance the rights, between authors and users, and between private and public interest. The balance between rights and exceptions/limitations in copyright is not an easy matter, particularly in light of ongoing technological developments and shifting of social and economic expectations, with respect to users and authors (Okediji, 2006).

## **2. Characteristics of the new scholarly environment**

### ***2.1 Socio-economic conditions***

Access to and management of information is imperative in contemporary society. Investing in information consists one of the most profitable economic activities. Indeed, information consumption tends to be directly or indirectly involved in every day life. Yamazaki (2007) claims that even when selling a T-shirt (a simple textile product) designers' fee or royalties on copyright make the 90-95% of the cost of the T-shirt. The prime cost of the cloth is estimated just at 5-10%. Such estimations have great implications to the work of libraries. Considering that libraries' work involves acquiring, managing and disseminating information, it can be assumed that intellectual property (IP) costs for libraries are enormous.

Commodification of information is indicated by many authors as a principal economic trait of the current era. Copyright industries are considerable economic powers today. In Britain, they represent at least 7% of GDP (Gross Domestic Product) (Taylor, 2007). The British book publishing industry generates yearly at least 5 billion GBP (British pounds), and the journal publishing another 1 billion GBP. The numbers are analogous in most developed countries of the world, where intellectual production is proliferating.

However, it has to be taken under consideration that a great amount of the income copyright industries are making comes from institutions such as universities and libraries, i.e. from public funding. It is worthwhile to refer an estimation made by the Society of College, National and University Libraries (SCONUL in Copyright and Research in the Humanities and Social Sciences, 2006), which mentions that only the administrative costs related to delays and difficulties in clearing rights, costs higher education institutions 30 million GBPs per year at a minimum. Furthermore, the contribution of copyright industries to the public welfare is strongly questioned as copyright laws protecting the economic interests of creators and rights owners restrict public access to the majority of copyrighted works. For these reasons, authors like Morrison (Morrison, 2008), talk about the

existence of two opposing social components, the “knowledge economy” and the “knowledge society”. For many, the liberation of information through open access initiatives and the decreasing of the copyright term which will transfer huge quantities of works into the public domain, are sought as the only chances for the advancement of democracy, culture, and learning.

## ***2.2 Education and research***

The role libraries come to play in education is a given in today’s societies, where the use of intellectual products is included in all curricula, and the existence of well equipped and organized libraries is a prerequisite for the accreditation of educational institutions. In most cases national copyright legislations provide for exceptions in the use of works for educational and teaching purposes. A good example of a well implemented copyright framework for the support of teaching and education is the US Technology, Education and Copyright Harmonization (TEACH) Act, which allows nonprofit academic institutions to use copyright protected material without the need to pay royalties or obtain permission from the owner. Although, there is the condition that the material should be reasonably used in terms of quantity (only some portions) and time (only for a specific period of time), the TEACH Act helped US academic institutions to support their educational programs with the appropriate bibliographical resources and provided students with the necessary access to important information.

However, the conditions change if the educational program is a paid one, i.e. students pay to attend it. In this case, the economic benefit that such a program may offer to the university becomes imperative and, thus, the use of copyrighted material may be considered as an infringement of copyright. At least this was the case in the print world, because in the new academic environment new forms of education and teaching are emerging such as distance education or e-learning, which require the whole of the educational material to be supplied in digital form, and, therefore, reproduction of copyrighted material is more intensively required than before.

Education is closely bound to, if not identical with, research, as a great part of research is conducted within academic institutions. Research involves the production of new ideas and therefore, the consumption -in terms of accessing, studying, and re-using- of copyrighted works. There are not many exceptions or limitations in the copyright law specifically concerning the use of materials for research purposes, as such an activity may fit in the general exception of “use in private study”. However, the British Academy (Copyright and Research in the Humanities and Social Sciences, 2006) states that “although there is no statutory definition of research, or clarity on what differentiates the use of otherwise copyright material in research from its use in private study, or in criticism, or in

review”, private study might represent only the consideration of existing ideas and not the invention of new ones as is the purpose of research. The same authority goes on by claiming that research in many cases is distinguished from research publication, but, “research without the publication of results is barely, if at all, distinguishable from private study and there is little or no public benefit in the production of new ideas unless they are made publicly available”.

The problem with research is that it may be characterized as “commercial”, if funded by private funds and, therefore, no copyright exceptions and limitations should be applied in commercial research study and publication. However, the majority of research involves public funding either in the form of financing or in the form of providing research equipment (installed in public institutions) or information resources (such as those held in public libraries), and the lack of access to its results could become a serious barrier to scholarship and social development in general. For these reasons, many national research institutions, such as the National Institutes of Health in the US or the Research Councils in UK have issued mandates that demand publicly funded research outcomes to become freely available either immediately or after a certain period of time that doesn’t exceed twelve months from the date of their first publication.

### **2.3 Digitization**

The ease of reproducing works with the help of new technologies --in the beginning, with the use of copying machines, and more recently, with the digitization of print material and the transmission via Internet of both digitized and electronically born content-- has alarmed creators and copyright owners. The situation has been aggravated with the massive digitization projects undertaken recently by libraries, but also private enterprises as Google.

Concerning libraries, which are the focal point of this paper, it has to be acknowledged that most copyright legislations provide libraries with the right to copy the material they hold in their collections for archival and preservation purposes. This exception to the right of reproduction usually involves certain preconditions, in order to be valid, such as: the material must be out of print and out of stock and cannot be re-purchased easily and in an affordable price. However, archival or preservation digital reproduction is not the goal in the current technologically advanced era. The goal is easy and immediate access to print or --preferably- digital material. Therefore, according to the European Bureau of Library, Information and Documentation Associations (EBLIDA, 2007), there is a need that the contents of libraries are digitized in order to enhance their availability for research, education and other non-commercial and commercial purposes. However, such a venture is not feasible within the current



copyright environment, especially considering that circa the 70% of all library materials are under copyright protection.

An important issue which comes to the fore in digitization projects and in the access to the digitized cultural content, is the so-called orphan works phenomenon. Orphan works are the works that the term of protection hasn't expired but the creator or the copyright owner cannot be identified or located. The questionable copyright framework of these works, a huge number of which is located in libraries, archives and museums, prevents many digital libraries -among them the European Digital Library- from achieving their goals (i2010: Digital Libraries Initiative). In order to find a solution for works, initiatives are undertaken both at European and global level (Commission of the European Communities, Green Paper, Copyright in the Knowledge Economy, Brussels, 16.7.2008, COM (2008) 466/3). Some countries, including Denmark and Hungary, have already established limitations in the use of such works while the creation of a global digital database is planned that will provide information on how to handle the variant cases of orphan works.

#### ***2.4 Public interest, access to information and knowledge, and fair-use***

The library community recognizes both the need of creators to be rewarded for their work and for creative works to be protected by the support of copyright, as well as the users' right to access information and knowledge. Both copyright and research and information rights are protected by national, European and international laws, and are closely associated with human personality and the cultural life of each and every region.

There are several conditions under the copyright legislation which prevent the public from freely accessing copyrighted material. Primarily, copyright legislation provides for the protection of creativity as expressed in any form of material and for the protection of creators against the abuse of their works. However in most legislations, also exists the counterbalancing idea of promoting new creativity as well as the progress of science also exists. This clearly indicates that copyright laws must not only be associated with the protection of creators or copyright owners, but also to cater for the good of the society. This is the reason why limitations to intellectual property rights and copyright exceptions are issued, so that certain levels of access are allowed to the public.

In copyright terms, these exceptions and limitations are also known as fair-use. As stated in a Public Policy Report issued by the Brennan Center for Justice (Heins and Beckles, 2005), fair-use is at risk today because aggressive and, sometimes irrational, claims by copyright owners cause many people to give up their fair-use

rights (Grodzinsky & Bottis 2007). In a research project conducted by the same institution, the definite conclusion was that artists and scholars have great interest in, but also, great confusion, on what fair-use is. A lot of scholars strongly complained about a copyright regime that prevents access to copyrighted material if the owner refuses permission or asks for very high charges.

In another report, a white paper issued by the Berkman Center for Internet and Society (Fisher and McGeeveran, 2006), four obstacles to educational use of content were indicated: a) unclear or inadequate copyright law relating to fair-use and educational use, b) extensive adoption of DRM-like technology to lock up content, c) practical difficulties in obtaining rights, and d) undue caution by copyright owners. All the above imply an urgent need for community advocacy and legal assistance in dealing with publishers, distributors, and other cultural gatekeepers, and libraries -as mediators between copyright owners and the public-have a central role in this issue.

According to the International Library Associations (eIFL, IFLA and LCA, 2009), the use of technological protection measures reduces the access to information and abolishes important national policies that were created for the public benefit. The World Intellectual Property Organization (WIPO) Copyright Treaty permits exceptions, but few countries have enacted exceptions for the benefit of libraries and library users. In the EC such a regulation is examined under the light article 6 paragraph 4, of the Directive 2001/29 and analyzed below.

## ***2.5 Scholarly communication and open access***

Scholarly communication stands in the heart of scientific evolution. According to a definition given by the UK Consortium of University and Research Libraries (CURL) and SCONUL (CURL and SCONUL in Ayris, 2005), scholarly communication is an umbrella term that “covers the authoring, publishing (in a broad sense), and reading of information produced by members of the academic community for teaching or research: ‘Information’ in this context may be in a variety of formats.” A central idea within scholarly communication is the re-using of scholarly publications for further developing science and stimulating new inventions. Academics are both authors and consumers of copyrighted material and in this sense, they are concerned with the rightful use of their works and, at the same time, they seek the highest possible dissemination and re-use of their publications by their peers.

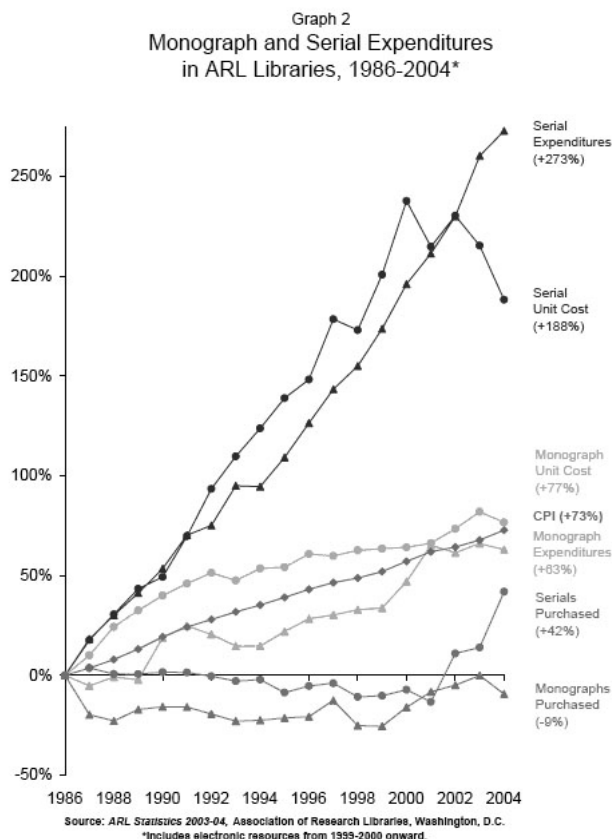
Open access initiative made its appearance in the beginning of the 21<sup>st</sup> century, and manifests the free access and availability of peer reviewed research publications to the public. “Open access literature is digital, online, free of charge, and free of most copyright and licensing restrictions. What makes it possible is the internet and the consent of the author or copyright-holder” and for this reason “it

does not require the reform, abolition or infringement of copyright law” (Suber, 2010). Open access is gradually gaining space among academics, researchers and librarians, and a major reason for its success is that it refers to scholarly publications, which do not represent a highly profitable and commercially exploitable intellectual product as music or movies.

There are two primary ways for exercising open access: a) through open access archives or repositories, which do not perform peer review, but simply make their contents freely available to the world, and b) through open access journals, which perform peer review, and then make the approved contents freely available to the world. Many academic publishers oppose to open access widespread adoption emphasizing on its negative impact on the relative economic sector (scholarly publishing industry). However, there is no reliable data yet to prove that such an impact exists. On the contrary, open access advocates stress the fact that the real loss comes from not moving to open access, as the lack of open access may result in a “constant and huge loss of efficient communication between scholars, and in particular the stifling of innovative interdisciplinary research and cross-discipline synergy of research” (Adams, 2007).

For many years, continuous and irrational increases in prices of scholarly books and journals in combination with shrinking library budgets due to financial constraints have driven libraries to reduce the number of their subscriptions and books purchases at a minimum, in many cases, level. As shown in Figure 1, the price of journals increased by 188% and that of monographs, by 77% during the Years 1986 to 2004. Further the reduce of subscriptions and monograph purchases had a severe impact on the amount of resources available to library users. As a response, libraries became pioneers in adopting the open access initiative as they were looking for less costly alternatives in order to continue to provide information services to their users. In this context, many academic libraries operate institutional repositories (IR) where scholarly publications accredited a University are deposited and openly available to the public. Open access to deposited material depends on the rights that authors can retain in order to shelf-archive their works either in personal web pages or in their institution’s IR. The role of copyright in the operation of such IRs is obvious.

Figure 1)



## 2.6 Libraries and the development of new services

With so many copyrighted works in their collections, libraries need to become experts in managing the use of their holdings in a lawful way. The role of librarians as a link between the producers of copyrighted material and consumers is very important. This role is twofold. On the one hand, librarians have to protect IP rights and reassure the legitimate use of print and electronic works held in their collections. On the other hand, librarians need to promote the right of people to access information and use it as a basis either for the creation of new works or for individual informational needs. To do that, librarians need to inform people about the exceptions and limitations of copyright legislation, and educate them on how to make the best and legitimate use of them.

Within the new academic environment as characterized by the advancement of open access to scholarly publications, librarians' educational and safeguarding role has been further expanded. Now, they are becoming the authors' consultants on how to publish in a way to achieve the highest levels of visibility and accessibility to their publications, how to self-manipulate the use of their works by implementing new licensing methods, such as creative commons, and how to advocate for the preservation of the fair-use doctrine in the digital world where easiness in controlling access to intellectual works can result in its shrinking.

### 3. The legal Framework

#### **3.1 Directive 2001/29/EC of the European Parliament and of the Council "on the harmonisation of certain aspects of copyright and related rights in the information society" and the Greek Copyright Law**

Copyright has an exclusive and absolute character, but is subjected to limits that are determined by the concept of the work or are explicitly prescribed by law as to the term and extent of the right. The scope of copyright comprises works as intangible goods, irrespective of the material on which the work is incorporated. The main features of a work are form and originality. The idea is not protected by copyright, unless it takes up a specific form. Copyright can only protect the form as stated in both national legislations and the International Berne Convention (article 2, §1). Copyright does not protect individual bibliographic citations, facts and headlines; although a collection of them would be protected by copyright and/or database right (Norman, 2004 Bottis 2006a). It should also be noted that protection does not extend to official texts that express the exercise of state power, especially legislative, administrative or judicial texts no to the expressions of folk tradition, news and simple events or facts, unless any of them can be included in the category of compilations or derivative works.

Apart from the conceptual limitations of copyright, the law imposes restrictions on the length of the right. According to the community *acquis*, the length of protection under national law is determined on the basis of the lifetime of the author and seventy years after his/her death. This length applies to both the moral and the property right. On expiry of this period, the work falls into the public domain.

And while the meaning of "fair-use" applies within the copyright system where certain indicative cases are provided which may be included within the meaning of "fair" and each case is judged ad hoc by the European system of IP, the limitations are numbered exclusively by the law, are applied exceptionally and have a narrow scope of application. In order to apply them, the jurist is called upon

to abide by the procedure of “the three-step-test”, that is to say, the application of the limitations only: a) in certain special cases; b) if there is no conflict with the normal exploitation of the work; and c) if there is no unreasonable prejudice of the legitimate interests of the author/right-holder. These criteria have been picked up as the bases for exceptions to rights in both the TRIPS (Trade-Related Aspects of Intellectual Property Rights) Agreement and the WIPO Copyright Treaty (WCT).

“The three-step-test”, is substantially the implementation of the article 9(2) of the Berne Convention and is regarded as the international yardstick for exceptions to exclusive rights. It is framed as a general provision that establishes the criteria against which any exception to the reproduction right is to be assessed. The proper interpretation of article 9(2) is a matter of some importance to national copyright legislators and policy makers, who are striving to fashion appropriate exceptions to protection in both the digital and non-digital environments (Ricketson, 2002).

The exceptions/limitations to the proprietary right relating directly or indirectly to libraries in the Greek legislation are provided in sections 18 to 28C of Law 2121/1993, as these apply after the incorporation of the European Directives (art. 5 par. 5 Directive 2001/29), the International Berne Convention (art. 9 par. 2), the TRIPS Agreement (art. 13) and the WIPO Copyright Treaty (WCT art. 10).

The provisions in relation to libraries are more detailed in legal systems outside the EU. In the USA for instance, the reproduction of works is allowed within the framework of non profitable libraries and archives, for various purposes, as private study and research, the restoration from theft or the maintenance in cases of defacing (Units 107 and 108 of the American law) (Crews, 2008).

The number of copies allowed is also expressly mentioned as well as the means of reproduction. Furthermore, there is a special provision for the last 20 years of the duration of protection, while the meaning of “fair-use” is very important. In the British Copyright, Designs and Patents Act 1988 (CDPA, 1998), there is a distinction made on whether the use is by a user of the material of the library or by the librarian.

In Directive 2001/29/EC “on the harmonisation of certain aspects of copyright and related rights in the information society” there is a closed catalogue of exceptions and limitations of which the only mandatory exception for member states is the one relating to temporary acts of reproduction within the use of networking applications such as the Internet. The remaining limitations are permissible exceptions and the member states chose whether they will incorporate them in their national legislations or not.

The limitations which refer to libraries and, generally to research and education, relate to:

- a) Special actions of reproduction carried out by libraries, educational establishments, museums or archives available to the public, which do not aim at any financial or commercial benefit.
- b) Uses with presentation or disposal for the purpose of research or private study through specialised terminals within the areas of the establishments mentioned above, provided they relate to works which do not fall under terms of sale or license and which are provided in their collections.
- c) Use as an example only during teaching or scientific research provided it is justified by the pursued non commercial purpose.
- d) Presentation of passages with the purpose of exercising criticism or book presentation.
- e) Uses for the benefit of persons with special needs directly connected to the disability and which do not have a commercial character.

### ***3.2 Reproduction right***

The Greek legislator choose not to use the possibilities afforded to it by article 5 (exceptions and limitations) of Directive 2001/29, a fact criticized by librarians and other beneficiaries. In relation to actions of reproduction within the framework of libraries, the Greek legislator could provide an exception in a more analytical content, taking into consideration their social function and not-for-profit nature. In any case, the actions of reproduction carried out within the libraries and in particular those of public educational institutions are actions of reproduction for private use of the person carrying them out (No. 18, Law 2121/93). There is no interaction of staff and the liability (as regards the scope of the reproduction) lies with the user him/herself. Actions of reproduction carried out by the staff of such libraries within the framework of rendering services also fall under this category, provided that they are reproductions of passages, relate to a small part of a work, are executed for the facilitation of private needs of the users and do not have any financial goals.

According to art. 5, par. 2 of Directive 2001/29, member states may provide for exceptions or limitations to the reproduction right of Article 2 in specific cases such as “in respect of specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage”. This exception for special actions of reproduction in museums, libraries etc is, in effect a particularisation of the more general exception for private use considered necessary by the

European legislator simply for the purpose of clarity. During the incorporation of the Directive in the Greek legal system, the inclusion of this exception in the amendments was not considered necessary exactly because there was and still is the general exception of reproduction for private use. That is to say, it was considered that the need referred to in exception 5.2 point c of this Directive was covered by the general section 18 of Law 2121/1993. However, because unjustified demands for payment of rights for this use have occurred, it is necessary now to incorporate this exception that there is longer any doubt about the legality, of the actions of reproduction within the libraries of the public educational institutions. In our view, Law 2121/1993 must include an expressed provision for the libraries of the public educational institutions of all levels and to refer exclusively to non profitable use.

Furthermore, the obligation of these libraries to post special notices within the areas of reproduction informing the users about the reasonable use of reproduction for personal use must be mentioned, ensuring firstly that the procedure of three stages is maintained, secondly that the spirit of the existing section 18 of Law 2121/93 is being followed while at the same time the ambiguity of law created by the lack of reference to certain categories of users is being lifted, and thirdly that the practice of certain states such as Spain (section 37(1) of the Spanish Law on Intellectual Property as amended by law No. 121/000044) or Portugal (section 75(2) of the Portuguese law No. 108/IX, as amended by law No. 50/2004) is applied but with the additional limitation of application only to a limited category of institutions such as that of libraries of public educational institutions of all levels.

According to art. 5, par. 3 of Directive 2001/29, the use "by communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals on the premises of establishments referred to in paragraph 2(c) of works and other subject-matter not subject to purchase or licensing terms which are contained in their collections" may be permitted. In our view, the Greek legislator must clearly adopt the mentioned exception for the libraries of public educational institutions. In order the law to evolve in parallel with contemporary technology and practices of remote access, the presentation or disposal of works must be allowed in all areas of educational institutions of all levels and must not be limited only to the area of the libraries of such institutions.

If the above exceptions for the libraries of public educational institutions of all levels are not adopted, then, apart from the financial issue of paying further rights to the creators of the works (or the collective management organizations -CMO- representing them) for the actions of reproduction and the lending of ma-



terial, the issue of previously granting a license reproduce and borrow by the creators or CMOs also occurs. It is understood that it is impossible for the libraries to handle such workload with the restricted number of staff they have, and the delays in securing such licenses shall result that any endeavour to satisfy the demands of a user will be futile.

According to art. 21 (Reproduction for teaching purposes) of Law 2121/1993 "It shall be permissible, without the consent of the author and without payment, to reproduce articles lawfully published in a newspaper or periodical, short extracts of a work or parts of a short work or a lawfully published work of fine art exclusively for teaching or examination purposes at an educational establishment, in such measure as is compatible with the aforementioned purpose, provided that the reproduction is effected in accordance with fair practice and does not conflict with the normal exploitation".

In our opinion, future amendments of Law 2121/93 must allow the reproduction of the digital content (born digital or digitized) for teaching purposes. Furthermore, it must be expressly mentioned that the exception includes contemporary forms of supporting actions to teaching, as coursepacks and e-reserves. Additionally, new methods of education, such as distance education and e-learning, must also be supported. These new educational methods are an emerging trend of huge practical and educational value. Distance learning cannot be legally covered by the existing status quo of Law 2121/1993, except via a private agreement. However, within the framework of WIPO, the discussion for possible exception relating to distance learning continues and may be introduced in Greek legislation via article 21 of Law 2121/1993. At the 17th Session of the WIPO Standing Committee on Copyright and Related Rights (SCCR), which took place in Geneva in 2008, the Committee welcomed the forthcoming study on exceptions and limitations for the benefit of educational activities, including distance education and the trans-border aspect thereof, in particular for developing and least developed countries.

According to art. 22 (Reproduction by Libraries and Archives) of Law 2121/93 «It shall be permissible, without the consent of the author and without payment, for a non profit-making library or archive to reproduce one additional copy from a copy of the work already in their permanent collection, for the purpose of retaining that additional copy or of transferring it to another non profit-making library or archive. The reproduction shall be permissible only if an additional copy cannot be obtained in the market promptly, and on reasonable terms». Therefore, the review of the existing legislation is deemed necessary in order to evolve in parallel with the contemporary technological demands relating to electronic/digital material, long term preservation. This procedure may need: multiple archival copies in electronic form (master record/derivative copies), digital substitutes,

mirror servers and different storage locations for securing maintenance of digital objects. Regular changes of the format of a digital object are constantly needed in order to continue being accessible depending on the technological evolutions etc. (Fragkou and Strakantouna, 2008).

### **3.2.1 Reproduction for the benefit of the blind**

For the visually impaired persons, or persons with other disabilities, there are many barriers to access knowledge and copyright is among them. The problem of accessing to knowledge for persons with disabilities is discussed at national and international level, and many organizations, as WIPO and UNESCO, are dealing intensively with the subject so as to find solutions. In this context various proposals to expand access to copyrighted works by persons who are blind or have other disabilities have been suggested (Sullivan, 2006; SCCR/19/3/2009; KEI, 2011 Bottis M., 2006b).

In the continuing dialogue among the European Union stakeholders a Memorandum of Understanding (MOU) was signed in order to: a) increase the access to works for people with print disabilities and, in the meanwhile, ensure that works converted into Braille or another accessible format, are available in other EU Member States through a network of Trusted Intermediaries, b) cross-border transfer in the EU of accessible copies created under copyright exceptions or under licenses, through a network of Trusted Intermediaries and under appropriate conditions is supported, and c) specific licenses allowing the cross-border transfer in the EU of licensed accessible copies, through the network of Trusted Intermediaries is achieved.

There is an indirect relation between libraries and the regulation allowing the reproduction of a work for the benefit of the blind or the deaf-mute for uses linked directly to their disability, and which do not have a commercial character. In Greece, the provision of the Copyright Law 2121/93 concerning the exception established for the benefit of blind and other disabled is included in the article 28A (Reproduction for the Benefit of Blinds and Deaf-mute) that provides that “the reproduction of the work is allowed for the benefit of blinds and deaf-mute, for uses which are directly related to the disability and are of a non-commercial nature, to the extent required by the specific disability. By Ministerial Order of the Minister of Culture the conditions of application of this provision may be determined as well as the application of this provision for other categories of people with a disability”. This provision was legislated in harmonisation to the Directive 2001/29 (art. 5 par. 3-b) and allows the determination of limits of its application by decision of the Minister of Culture, as well as its extension to other categories of persons with disabilities.

In 2007 with the Ministerial Order (ΥΠΠΟ/ΔΙΟΙΚ/98546) «reproduction of copyrighted work for the benefit of the blind and the deaf-mute and extensions of the arrangement to other categories of people with disabilities», the Greek State tried to facilitate their access to information by establishing an obligation for the publishers, to deliver to the competent intermediary bodies the files of the works to be reproduced in electronic format (Papadopoulou, 2010).

### **3.3 Public lending**

The rental and lending legislation has affected library services and the lending of copyrighted books, artistic materials, CD-ROMs, computer software etc. Authors, artists, dramatists, composers, performers and producers of sound and video recordings, as well as producers and principal directors of films, have the exclusive right to authorize or prohibit rental and lending of their works.

According to the current European law, public lending can be defined as the act of “making available for use, for a limited period of time and not for direct or indirect economic or commercial advantage, when it is made through establishments which are accessible to the public”. This definition is provided by article 2.1 b) of the Directive 2006/115/EC “on rental right and lending right and on certain rights related to copyright in the field of intellectual property”.

According to the PLR (Public Lending Right) International Network, 29 nations now have working PLR systems. At least 23 other countries have PLR in their legislation but have still to take the next step towards establishing operational systems. The latter group includes countries as widely scattered as: St Lucia, Samoa, Burkino Faso, FYROM (Former Yugoslav Republic of Macedonia) and Mauritius. The implementation of the PLR is a very complex issue and the most common loan-based PLR became practicable when the invention of modern sampling and computer processing made it so (Strakantouna and Kikkis, 2010).

At European level, the PLR has been harmonized in 1992 with the Directive 92/100/EEC. According to art. 5 of the Directive 92/100/EEC and to art. 6 of the latest Directive 2006/115/EC: a) Member States may derogate from the exclusive right provided for in Article 1 in respect of public lending, provided that at least authors obtain remuneration for such lending, b) where Member States do not apply the exclusive lending right provided for in Article 1 as regards phonograms, films and computer programs, they shall introduce, at least for authors, a remuneration and c) Member States may exempt certain categories of establishments from the payment of the remuneration referred to in paragraphs 1 and 2. In spite of these abilities the Greek legislator does not make full use of the derogation from the exclusive right. This fact was criticized not only by the library but also by the law community (Marinos, 1998; Papazoglou, 2006). Therefore, in

Greece the PLR maintain an exclusive character, where libraries and institutions that lend copyrighted works in order to be legitimate, have the obligation to ask permission from the creator or the copyright holder in order to be legitimate. The employment of PLR is not regulated by law or other special administrative order but has been left to the creators and the collective societies (Kallinikou, 2007).

In our opinion the Greek legislator must take advantage of possibilities given by the Directive and adopt with clarity an exception for libraries of public educational institutions of all levels for the promotion of education and learning. It is important to point out that such a provision serves a number of conditions:

- a) It is within the limits of article 6 of Directive 2006/115EC.
- b) It is in accordance with the decisions of the Court of Justice of the European Union, because while it uses the possibility of nominating certain institutions exempted from the payment of right according to article 6 of Directive 2006/115 EC, it refers to a very limited and specific category of institutions, that is to say, the libraries of public educational institutions and not all public libraries. As a consequence, it is in accordance with the decisions of the Court of Justice of the European Union (e.g. The case of the Commission of Europe v. the Belgian Republic C-433/02 or the case of the Commission of Europe v. the Portuguese Republic C-53/05).
- c) It is an expression of the public and free character of education in Greece and it is in accordance with the mission of the libraries of public educational institutions of all levels (Fragkou and Strakantouna, 2008).

Furthermore, the low use of libraries and library services in Greece (frequency of library visits, circulation of library material), as indicated in the 3<sup>rd</sup> Pan-Hellenic Survey of Reading Behaviour and Cultural Practices, conducted by the National Book Center of Greece in December 2010, elevates any concerns that authors, rights holders and/or publishers might face considerable financial loss from low books sales caused by the public lending services offered by libraries.

### ***3.4 Towards a common framework for limitations and exceptions***

Many studies about models and practices concerning copyright exceptions and limitations in the digital environment have been developed. All these studies determine that exceptions and limitations for libraries are needed in order to promote creation, innovation, and dissemination of knowledge, and they suggest that a minimum agreement on core exceptions and limitations is required in all national legislations. Between years 2003-2010 the WIPO SCCR have been studying and illustrating most of these models and practises that lay emphasis to the issues of visually impaired, libraries and archives, educational activities etc. With-

in this context, Kenneth Crews, commissioned by WIPO, published in 2008 his *“Study on Copyright Exceptions and limitations for Libraries and Archives”*. The study is the first comprehensive overview of statutory provisions in national copyright laws of WIPO Member States for the benefit of libraries and archives. According to this study, the 184 from the totality of 184 WIPO countries have at least one statutory library exception, most of the countries have multiple statutes addressing a variety of library issues, whereas 21 countries have no library exception in their copyright law (Grews, 2008).

The outcomes of the 21st Session of the WIPO SCCR in November 2010 were characterized by IFLA as “unprecedented opportunity for libraries and archives” because at this meeting WIPO agreed on a work program that could lead to an international treaty involving mandatory exceptions for the benefit of users of copyrighted works, heralding a new era for copyright in the 21st century. More specifically, they agreed for a work plan until the end of 2011 concerning copyright exceptions and limitations for libraries and archives, educational, teaching and research institutions, and persons with other disabilities (IFLA, 2010).

The international library community promotes the necessity of adoption of more copyright exceptions and specific provisions in the copyright law. In May, IFLA announced a statement on copyright exceptions and limitations for libraries and archives. Through this statement it asks WIPO to take actions so that member states adopt in their laws provisions the following specific principles helping the effectiveness of libraries’ and archives’ activities:

- a) For preservation purposes libraries and archives should be permitted to make copies of published and unpublished works in its collections, including migrating content to different formats.
- b) Libraries and archives should be able to support interlibrary loan and document delivery, directly or through the intermediary library irrespective of the format and the means of communication.
- c) Reproduction and copying individual items for or by individual users should be permitted for research and study and for other private purposes.
- d) A library should be permitted to convert material from one format to another to make it accessible to disabled persons. So the exception for them should apply to all formats to accommodate user needs and technological advances.
- e) A library or educational institution should be permitted to make copies of a work in support of classroom teaching.
- f) A general free use exception consistent with fair practice ensures the effective delivery of library services.

- g) Legal deposit laws and systems should be broadened to include works published in all formats allowing copying or downloading of those works.
- h) An exception is needed to resolve the problem of orphan works, where the rights holder cannot be identified or located.
- i) Copyright term consistent with the Berne Convention and the TRIPS Agreement, the general term of copyright should be the life of the author plus 50 years.
- j) Provisions that should be permissible for libraries and their users to circumvent a technological protection measure for the purpose of making a non-infringing use of a work.
- k) Contracts should not be permitted to override exceptions and limitations. The goals and policies providing for exceptions are important statements of national and international principle and should not be varied by contract.

Finally, there should be a limitation on liability for libraries and library staff who act in good faith, believing or having reasonable grounds to believe, that they have acted in accordance with copyright law (EIL, IFLA, WIPO SCCR, 2009).

#### 4. Epilogue

In order to find a balance between the needs of libraries and archives, creators, copyright holders and users, moderate forms of cooperation such as codes of conduct, protocols of cooperation, agreements, or even collective agreements are being tried. However, the existence of a suitable legal framework which balances the interests of the beneficiaries and the public is considered of paramount importance, especially for organizations serving educational, research and cultural purposes.

#### References

3<sup>rd</sup> Pan-Hellenic Survey of Reading Behaviour and Cultural Practices (2010), National Book Center of Greece. Online at <<http://www.ekebi.gr/frontoffice/portal.asp?cpage=RESOURCE&cresrc=8433&cnode=309>, accessed 07/04/2011>.

Adams, A.A. (2007), Copyright and research: an archivangelist's perspective, SCRIPT-ed, 4(3). Online at <<http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/adams.pdf>, accessed 21/01/2011>.

Ayris, P. (2005), The scholarly communications revolution: information tools and content in a global and institutional setting, presented at: ICAU '05: 16th International Consortium of Aleph Users and International SFX/MetaLib User Group Conference, London, UK, online at <[http://discovery.ucl.ac.uk/4904/1/Ayris\\_ICAU05.pdf](http://discovery.ucl.ac.uk/4904/1/Ayris_ICAU05.pdf), accessed 10/03/2011>.

Bottis M., Access to Information for People with disabilities, *Ionian Law Review*, December 2006, issue 6, pp. 34-48.

Bottis M., Copyright and exceptions of education and teaching, *Modern Education*, 2006, pp. 86-102 (in Greek).

Copyright and Research in the Humanities and Social Sciences: a British Academy review, September 2006. Online at <<http://www.britac.ac.uk/templates/asset-relay.cfm?frmAssetFileID=6389>, accessed 21/01/2011>.

Copyright and the digitisation of library materials: discussion paper for the meeting between EBLIDA and FEP, June 2007.

Copyright, Designs and Patents Act 1988 (CDPA). Online at <<http://www.legislation.gov.uk/ukpga/1988/48/contents>, accessed 12/04/2011>.

Crews, K. (2008), Study on copyright limitations and exceptions for libraries and archives, Standing Committee on Copyright and Related Rights. Online at <[http://www.wipo.int/edocs/mdocs/copyright/en/sccr\\_17/sccr\\_17\\_2.pdf](http://www.wipo.int/edocs/mdocs/copyright/en/sccr_17/sccr_17_2.pdf), accessed 12/04/2011>.

eIFL, IFLA and LCA (2009), Statement of principles on copyright exceptions and limitations for libraries and archives, WIPO SCCR, 18<sup>th</sup> Session, Geneva, May 25-29, 2009. Online at <<http://www.ifla.org/files/clm/statements/statement-of-principles-sccr20.pdf>>. Accessed 12/04/2011.

Fischer, W.W. and McGeveran, W. (2006), The digital learning challenge: obstacles to educational uses of copyrighted material in the digital age: a foundational white paper, The Berkman Center for Internet & Society at Harvard Law School, Research Publication No. 2006-09. Online at <<http://cyber.law.harvard.edu/media/files/copyrightandeducation.html>>, accessed 15/03/2011.

Fragkou, A. and Strakantouna, V. (2008) proposals to the Hellenic Library Association in the context of negotiations with the Hellenic Copyright Organization (OPI). (unpublished).

Grodzinsky F. & Bottis M., Private Use as Fair Use: Is it Fair? *ACM SIGCAS Computers and Society* vol. 37 issue 2 November 2007.

Heins, M. and Beckles, T. (2005), Will fair use survive? Free expression in the age of copyright control: a public policy report, Brennan Center for Justice at NYU School of Law. Online at <<http://www.fepproject.org/policyreports/Will-FairUseSurvive.pdf>, accessed 15/03/2011>.

i2010: Digital libraries initiative. Online at <[http://europa.eu/legislation\\_summaries/information\\_society/i24226i\\_en.htm](http://europa.eu/legislation_summaries/information_society/i24226i_en.htm)>, accessed 10/03/2011.

IFLA, Press Release 19 November 2010 "Unprecedented opportunity for libraries and archives" - WIPO to work on library and archive copyright exceptions. Online at <<http://www.ifla.org/en/news/unprecedented-opportunity-for-libraries-and-archives-wipo-to-work-on-library-and-archive-copyri>>, Accessed 12/04/2011.

Kallinikou, D. (2007), Intellectual property and Libraries. Online at <<http://www.ipr-online.org/unctadictsd/docs/ruth%202405.pdf>>, accessed 12/04/2011. (In Greek).

Knowledge Ecology International (KEI) (2011), Background and update on negotiations for a WIPO copyright treaty for persons who are blind or have other disabilities. Submitted by James Love. Online at <<http://keionline.org/node/1089>>, accessed 12/04/2011.

Marinos, M.-T (1998), Some notes upon the status of traditional libraries and public digital libraries under the system of Law 2121/1993, Hellenic Justice Magazine (EllDik) 1998. (In Greek).

Morrison, H. (2008), Summary and conclusions. Final chapter of Scholarly Communication for Librarians, 2008. In Scholarly Communication for Librarians, Chandos. Online at <<http://hdl.handle.net/10760/13178>>, accessed 09/03/2011.

Norman, S. (2004), Practical Copyright for information professionals, Faced Publishing.

Okediji, R. L. (2006), The international copyright system: limitations, exceptions and public interest. Online at <[http://www.unctad.org/en/docs/iteipc200610\\_en.pdf](http://www.unctad.org/en/docs/iteipc200610_en.pdf)>, accessed 12/04/2011.

Papadopoulou, M.D. (2010), Copyright exceptions and limitations for persons with print disabilities: the innovative Greek legal framework against the background of the international and European developments, Proceedings, 3rd International Seminar on Information Law, An Information Law for the 21st century, Nomiki, Athens 2010, pp. 348-387.

Papazoglou, V. (2006), Horizontal Action of Academic Libraries: legal issues, Proceedings of the Conference Minutes, Archives, Libraries and the Law in the era of Information Society, Athens, February 2-3, 2006, National Library of Greece.

Pedley, P. (2007), Digital copyright, Faced Publishing, 2nd ed.

Public Lending Right (PLR) International. Online at <http://www.plrinternational.com/>>. Accessed 15/03/2011.

Ricketson, S. (2002). The three-step-test, deemed quantities, libraries and closed exceptions, A study, Centre for Copyright Studies.



Ridley, M. (2005), Digital libraries and new technologies: exploring roles and dislocations, University of Western Ontario, November 22, 2005. Online at <<http://www.uoguelph.ca/~mridley/digital-libraries/UWO-Nov2005.ppt>>, accessed 15/03/2011.

Strakantouna, V. (2010), Privacy in libraries: the coexistence of ethical principles and legal rules, Proceedings of the 3rd International Seminar on Information Law, Corfu, Ionian University, An Information Law for the 21st Century, Nomiki Vivliothiki, pp. 490-501.

Strakantouna, V. and Kikkis, G. (2010), The two-fold purpose of public lending right, Proceedings of the 19th Hellenic Conference of Academic Libraries organized by the Library and Information Service of the Panteion University in Athens "Scientific communities and libraries in a world of social networking and synergies.

Suber, P. (2010), Open access overview: focusing on open access to peer-reviewed research articles and their preprints. Online at <<http://www.earlham.edu/~peters/fos/overview.htm>>, accessed 05/01/2011.

Sullivan, J. (2006), Study on copyright limitations and exceptions for the visually impaired, prepared for WIPO SCCR 15th Session, SCCR/15/7. Online at <[http://www.wipo.int/edocs/mdocs/copyright/en/sccr\\_15/sccr\\_15\\_7.pdf](http://www.wipo.int/edocs/mdocs/copyright/en/sccr_15/sccr_15_7.pdf)>, accessed 12/04/2011.

Taylor, K. (2007), Copyright and research: an academic publisher's perspective, SCRIPT-ed, 4(2). Online at <<http://www.law.ed.ac.uk/ahrc/script-ed/vol4-2/taylor.pdf>>, accessed 21/01/2011.

Yamazaki, H. (2007), Changing society, role of information professionals and strategy for libraries, IFLA Journal 33(1). Online at <<http://ifl.sagepub.com/content/33/1/50>>, accessed 09/03/2011.

# RIPE NCC - Internet governance and registration of IP addresses

---

---

Athina Fragkouli

---

---

## 1. Introduction

### *1.1 Internet Protocol and IP addresses*

The Internet started as an experimental project in the late 1960s by US government-funded researchers. These researchers saw great potential value in allowing computers located in different geographic locations to remotely communicate with each other. In the early days the Internet was named ARPANET and connected research networks located in Universities and Research Institutes, mainly in the United States<sup>1</sup>.

The architecture of the Internet is based on a system named the Internet Protocol (IP) that was formally documented in 1981. The Internet Protocol is designed to allow communication between interconnected networks. This communication is achieved by transmitting packets of data between devices in these interconnected networks.

For the purposes of routing the data to be transmitted from device to device, the location of each device must be uniquely identified within these networks. Therefore each device is given a unique address, known as Internet Protocol (IP) address<sup>2</sup>.

The Internet Protocol documented in 1981 is called Internet Protocol version 4 and the IP addresses within this protocol are named IP version 4 (IPv4) addresses. IPv4 addresses consist of 32 bits and they appear as 4 numbers (from 0 to 255) separated by dots (for example 192.0.2.76). This combination generates over four billion IPv4 addresses, which in 1981 appeared to be enough for the needs of the limited networks participating in the Internet.

- 
1. For more information see Leiner B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., Wolff, S., A brief history of the Internet, online at <<http://www.isoc.org/internet/history/brief.shtml>>accessed 18.04.2011.
  2. Postel J., (1981) Internet Protocol DAPRA Internet Program Protocol Specification, RFC 791, online at <<http://www.ietf.org/rfc/rfc791.txt>> accessed 18.04.2011.

The unexpected success of the Internet though, made the number of the possible IPv4 addresses insufficient for the needs of the continuously increasing number of networks globally. In the 1990s a new version of the Internet Protocol was designed as a successor to the IPv4 protocol.

IP addresses based on the Internet Protocol version 6 (IPv6 addresses) are 128-bit numerical identifiers instead of the 32-bit addresses provided by the IPv4 protocol.<sup>3</sup> That means that the number of IP addresses produced by the IPv6 protocol are  $2^{128}$  individual addresses available, which is approximately  $3.4 \times 10^{38}$ , and exactly: 340,282,366,920,938,463,374,607,431,768,211,456 IP addresses.<sup>4</sup>

### ***1.2 Need for cooperation and coordination among network operators***

As the use of the Internet expanded beyond geographic limits and its applications expended beyond research or governmental needs, network operators realised the need to coordinate with each other and to create policies and procedures for the proper function of the Internet.

This paper explains Internet governance with regards to the registration of IP addresses as deployed over the years by the network operators from across the world. It analyses the reasoning behind the creation of the Regional Internet Registry system, the structure and the function of the Regional Internet Registries in general and of the RIPE NCC in particular as the Regional Internet Registry in Europe, Middle East and Central Asia. Furthermore the paper presents the policy-making procedure that generates the policies according to which Regional Internet Registries operate. Finally, it will examine the principles according to which IP addresses are distributed and registered to networks, the function and the importance of the publicly available registry (also known as the RIPE database) and future challenges for this system.

## **2. Internet governance**

### ***2.1 Development of the Internet Registries concept***

Communication between devices using the Internet Protocol relies on identifying the appropriate devices; IP addresses serve the purpose of identifying devices in a network. Therefore IP addresses have to be unique. To ensure that a unique IP address is attached to each device, IP addresses must be distributed and registered

---

3. Deering S., Hinden R., (1998), Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, online at <http://www.ietf.org/rfc/rfc2460.txt/> accessed 18.04.2011.

4. RIPE NCC, What is IPv6?, online at <http://www.ipv6actnow.org/info/what-is-ipv6/> accessed 18.04.2011.

in an organised manner. This requirement was identified from the early years of the Internet.

Initially, it was one person, named Jon Postel, who registered in a notebook the IP addresses distributed to networks that wanted to become connected to the Internet. Later, at the beginning of the 1990s, this function was formally transferred to the Internet Assigned Numbers Authority (IANA).<sup>5</sup>

As the Internet in the early years was a research project, organisations that requested IP addresses for their networks were generally those participating in the research effort, such as military, government and government-sponsored research organisations. Moreover, due to the fact that the Internet was a project originally funded by the US government, the criteria for assigning IP addresses were based on US federal laws.

As the Internet became more stable though, it started being used by a broad range of academic and research institutions as well as by the industry. Additionally the use of the Internet was increasing and being developed in a wide geographical area. Organisations from different countries were requesting the assignment of IP addresses in order for their networks to be interconnected. Applying the same criteria to all network operators without taking into account the individual needs of different networks in the various geographic regions was considered inappropriate.

Network operators concluded that allocation and registration criteria could not be harmonized globally by one single organisation and therefore IANA was regarded as unable to handle the distribution of IP addresses for diverse stakeholders in different geographic regions. The need for a new system of allocation and registration of IP addresses was defined, which would meet the demands of network operators in different regions.

In 1990, a new system was proposed.<sup>6</sup> This new system suggested the creation of an Internet Registry that would be responsible for the allocation and the registration of IP addresses. The function of this Internet Registry would be distributed among multiple centers on different geographic regions.

IP addresses would be allocated and registered according to criteria determined by the specific needs and the particularities of the relevant stakeholders in each

---

5. More information about Jon Postel can be found online at <http://www.isoc.org/awards/postel/memory.shtml> /accessed 18.04.2011.

6. Cerf V., (1990), IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet «Connected», RFC 1174, online at <http://www.rfc-editor.org/rfc/rfc1174.txt> /accessed 18.04.2011.

geographic region. These criteria would be defined by the administrators of the networks located in each particular region. In other words, network operators themselves would be able to determine the particular criteria according to which IP addresses would be assigned to them.

Finally, the Internet Registry would also collect and administer information that would be publicly available for the purposes of permitting network administrators to make decisions as to the acceptability of traffic destined to or from each and every legitimate IP address.

Over the next two years, the need for the distribution of the registration function became urgent as the demand for IP addresses grew significantly. In 1992 a plan was developed for the implementation of the 1990 proposal regarding the management of the distribution and registration of IP addresses.<sup>7</sup>

According to this plan the distribution and registration of IP addresses for different geographic regions would be managed by different Regional Internet Registries (RIRs). It was crucial, according to the plan, that allocation and registration of IP addresses in each geographic region would be managed by a single RIR. The basic criterion for the qualification of an organisation as an RIR would be the relevant recognition and support expressed by the networks operator within the geographic area the RIR was meant to be responsible for. In other words it was crucial that this organisation would be unbiased and widely recognised as an RIR by network providers within the respective geographic region.

## ***2.2 The developments in Europe - RIPE and the RIPE NCC***

Parallel to this development, in Europe a group of Internet pioneers acknowledged the necessity of creating a forum where all network operators in Europe and beyond would be able to cooperate technically in order to promote and coordinate interconnection of IP networks within Europe as well as with networks on other continents and to exchange relevant information. This forum was created in 1989, and named Réseaux IP Européens (RIPE)<sup>8</sup>. It began a series of regular meetings to share experiences and carry out technical coordination work. Additionally the group started exchanging information for coordinating purposes and established a publicly available database for storing operational data. This data-

---

7. Gerich E., (1992), Guidelines for Management of IP Address Space, RFC 1366, online at <http://www.rfc-editor.org/rfc/rfc1366.txt>/accessed 18.04.2011.

8. Blokzijl R., Brunel M., Fluckiger F., Karrenberg D., Martin O., Valente E., (1992), RIPE Terms of Reference, ripe-001, online at <http://www.ripe.net/ripe/docs/ripe-001>/accessed 18.04.2011.

base was initially referred to as a “whois database” because it consisted information about the networks that have been distributed IP addresses to.

The RIPE community was following closely and participating in the discussions about the creation of an Internet Registry and the distribution of its function to Regional Internet Registries for different geographic regions. In 1990, the RIPE community proposed the creation of a Network Coordination Center for the support and coordination of the management of a pan European IP network. This Network Coordination Center would act as the Regional Internet Registry for IP addresses in Europe and in this way it would contribute to the global administrative framework of the Internet.

This Network Coordination Center was founded in 1992 and was named the RIPE Network Coordination Center (RIPE NCC) and since then it has kept the registry of IP addresses allocated in Europe, Middle East and Central Asia.<sup>9</sup>

### ***2.3 The Regional Internet Registry system***

In 1996 a Best Current Practice document was approved, which provided general rules and guidelines governing the distribution and registration of IP addresses.<sup>10</sup> This document defined the RIR system by describing its structure, the hierarchy of the stakeholders in this system and their relationships with each other.

On the top of this hierarchy IANA was established as the authority over all IP addresses used in the Internet. IANA would allocate blocks of these IP addresses to Regional Internet Registries.

At a second level the Regional Internet Registries would be established under the authority of IANA and would operate in large geopolitical regions such as continents. The RIPE NCC was recognised in this document as the Regional Internet Registry for Europe and other areas.<sup>11</sup>

At a lower level Local Internet Registries would be established under the authority of the Regional Internet Registry in their respective region and IANA. Local Internet Registries would be responsible for the distribution and registration of

---

9. Blokzijl R., Devillers Y., Karrenberg D., Volk R., (1990), RIPE Network Coordination Center (RIPE NCC), ripe-19, online at <ftp://ftp.ripe.net/ripe/docs/ripe-019.txt>/accessed 18.04.2011.

10. Hubbard K., Kusters M., Conrad D., Karrenberg D., Postel J., (1996), Internet registry IP allocation guidelines, RFC 2050, online at <http://www.ietf.org/rfc/rfc2050.txt>/accessed 18.04.2011.

11. Later the RIPE NCC was recognised by the European Union. For more information see [http://ec.europa.eu/information\\_society/policy/internet\\_gov/index\\_en.htm/](http://ec.europa.eu/information_society/policy/internet_gov/index_en.htm/) accessed 18.04.2011.

IP addresses to network operators. However Local Internet Registries would be coordinated and represented by their relevant Regional Internet Registry.

The Best Current Practices of 1996 also stipulated the establishment of a public registry documenting address space allocation and assignment. This would be necessary to ensure uniqueness and to provide information for Internet trouble shooting at all levels. The RIPE NCC was already adhering to this condition by maintaining the “whois database”, which was called RIPE Network Management Database and later on RIPE Database.

## ***2.4 Establishment of RIRs and the Number Resources Organization (NRO)***

Initially the criteria for an organisation to become an RIR were not specifically defined. It was however crucial that the Internet community of a specific region support the establishment of a certain organisation as the Regional Internet Registry for their region.<sup>12</sup> This was the case for example with the RIPE NCC, which was established with the support of the RIPE community that represents the Internet community in that region.

Later on, ICANN<sup>13</sup> published a document that defined concrete criteria for the establishment of new Regional Internet Registries based on the following principles<sup>14</sup>:

- 1) the region of coverage by the proposed Regional Internet Registry should meet a concrete scale to be defined by ICANN, in order to avoid fragmentation of IP address blocks
- 2) the proposed Regional Internet Registry must be broadly supported by Local Internet Registries in the proposed region
- 3) there must be an established bottom-up self-governance structure for setting local policies (see below for RIPE policies)
- 4) the proposed Regional Internet Registry must be neutral and impartial in relation to all interested parties, and particularly the Local Internet Registries in the relevant region

---

12. See above, Hubbard K., Kusters M., Conrad D., Karrenberg D., Postel J., (1996), Internet registry IP allocation guidelines, RFC 2050.

13. Internet Corporation for Assigned Names and Numbers (ICANN) is the organisation that in undertook the IANA function in 1998. For more information see <http://www.icann.org/en/participate/what-icann-do.html> /accessed 18.04.2011.

14. ICANN, (2001), ICP-2: Criteria for Establishment of New Regional Internet Registries, online at <http://www.icann.org/en/icp/icp-2.htm> / accessed 18.04.2011.

- 5) the proposed Regional Internet Registry must have a staff of technical experts
- 6) the proposed Regional Internet Registry must adhere to global policies regarding address space conservation, aggregation and registration<sup>15</sup>
- 7) the proposed Regional Internet Registry must have a clear activity plan
- 8) the proposed Regional Internet Registry must have a funding model
- 9) the proposed Regional Internet Registry must have a system for keeping records so it operates as a registry
- 10) all business information it receives from Local Internet Registries must be treated as confidential.

Until now five organisations fulfill the criteria as set up in the above document:

- AfriNIC, for the African region
- APNIC, for the Asian Pacific region
- ARIN, for North America and some Caribbean Islands
- LACNIC, for Latin America and some Caribbean Islands, and
- RIPE NCC for Europe, Middle East and Central Asia (former U.S.S.R.)

RIRs are independent from each other and represent different service regions. They are not competing each other, rather they cooperate with each other because they are all parts of the global Internet registration system. In 2003 they formed the Number Resource Organization (NRO), the purpose of which is to serve as the coordinating mechanism of the RIRs for acting collectively on matters relating to the interests of the RIRs, such as the promotion and protection of the bottom-up policy development process. Additionally the NRO is meant to be the point of reference for input from the multistakeholder Internet community regarding the RIR system.

The NRO is not incorporated to a legal entity. According to the Memorandum of Understanding of all RIRs for the creation of the NRO, “[a]ny legal obligations incurred or undertakings made by the NRO either in its unincorporated status, or once incorporated, shall require the prior written commitment of all RIRs through the signature of all RIR CEOs.”

---

15. The concepts of address space conservation, aggregation and registration are explained in section 3.1. of this paper.



## **2.5 Legal framework of the RIPE NCC**

### **2.5.1 Structure of the RIPE NCC**

The RIPE NCC, like all Regional Internet Registries, is a non-for-profit organisation. In particular the RIPE NCC is an association under Dutch law. It consists of the following bodies:

- The individual Members: members of the RIPE NCC can be natural or legal persons.
- The General Meeting: this is the core of the RIPE NCC. The General Meeting of the Members takes the most important decisions such as the adoption of the activity plan and recommendation on the budget.
- The Executive Board: the Executive Board is elected by the General Meeting and consists of five individuals.
- The Management Team: the technical team to which is delegated the day to day activity of the RIPE NCC.

### **2.5.2 Contractual relationships with LIRs and End Users**

Every network operator who receives IP addresses in the RIPE NCC service region is bound by a contract. This section presents the different kinds of contractual relationships within the RIPE NCC service region.

As described above, Regional Internet Registries delegate the distribution of IP addresses on a local level to Local Internet Registries (LIRs). LIRs within the RIPE NCC structure are natural or legal persons that receive IP addresses and related services based on a contract with the RIPE NCC. LIRs are in principle Members of the RIPE NCC and they must pay an annual fee as contribution to the RIPE NCC activities. It must be highlighted however that this fee does not specially refer to the allocation of IP addresses, but to the provision of RIPE NCC services in general.<sup>16</sup>

LIRs sub-allocate IP addresses to their customers. Within the RIR system these customers are known as End Users. This sub-allocation is usually subject to a contract between the LIR and the End User. The End Users are not necessarily the individual users of a device connected to the Internet through an IP address. In fact End Users are generally organisations that request IP addresses in order to

---

16. RIPE NCC Standard Service Agreement, (2008), online at <https://www.ripe.net/ripe/docs/ripe-435> / accessed 18.04.2011, RIPE NCC Standard Terms and Conditions, (2008), online at <https://www.ripe.net/ripe/docs/ripe-418> / accessed 18.04.2011, RIPE NCC Charging Scheme, (2011), online at <http://www.ripe.net/ripe/docs/ripe-499> / accessed 18.04.2011.

connect their network to the Internet without having any interest in acting as a local Internet registry by sub-allocating parts of their allocation to any other organisations further on.

For technical reasons, End Users that receive IP addresses sub-allocated from an LIR's allocation are not able to manage the network attached to these IP addresses independently from the LIR. End Users who want to manage their network independently from an LIR, can request IP addresses from the RIPE NCC directly or indirectly through an LIR, in which case the LIR will only forward the request to the RIPE NCC without sub-allocating IP addresses from their own allocation. This way End Users are able to manage their network independently from an LIR. The End Users that want this independent management of IP addresses have to conclude a contract with either the RIPE NCC or the LIR accordingly.<sup>17</sup>

## ***2.6 RIPE policy-making process – a self-regulatory system***

The system according to which the RIPE NCC distributes IP addresses is determined by policies adopted by the RIPE community, which are named RIPE policies. There is a clear functional distinction between the RIPE NCC and the RIPE community. The RIPE NCC does not make the RIPE policies; the RIPE community makes them. The RIPE NCC is responsible for the implementation of the RIPE policies.

There is also a distinction between Members of the RIPE NCC and participants of the RIPE community. Members of the RIPE NCC have to pay a fee to contribute to the activities of the RIPE NCC. Participants of the RIPE community do not have to pay any fees in order to participate in the discussions and in the policy-making process of the RIPE community. Being a Member of the RIPE NCC is not incompatible with being a participant of the RIPE community. In fact, Members of the RIPE NCC often participate in the discussions and the policy-making process of the RIPE community. However, participants of the RIPE community do not have to be Members of the RIPE NCC.

The policies adopted by the RIPE community define the criteria according to which the RIPE NCC distributes and registers IP addresses. To make sure that these criteria represent the particular needs of all relevant stakeholders in the region RIPE NCC is responsible for, the RIPE policy-making process presents the following characteristics:

---

17. Hilliard N., (2009), Contractual Requirements for Provider Independent Resource Holders in the RIPE NCC Service Region, online at <http://www.ripe.net/ripe/docs/ripe-452/> accessed 18.04.2011.

- It is open for everyone to participate. It represents anyone having an interest in participating in the policy-making procedure.
- It is transparent.
- It follows a bottom-up process.
- The decision making process is based on consensus.<sup>18</sup>

The following section will analyse these aspects.

## Openness

The RIPE community is a forum without legal personality, formal membership, or any participation fees. RIPE community is open to anyone who wants to participate in the policy-making procedure and the relevant discussions. This way, policies made by the RIPE Community are representative of the actual needs and requests of those they are applicable to.

To participate in the discussions and the policy-making process of the RIPE community, people can subscribe to the mailing lists created for these purposes.<sup>19</sup> Subscription to these mailing lists is open to everyone and free. Discussions are also taking place in meetings of the RIPE community (RIPE Meetings). These meetings are also open for everyone to participate physically or remotely. Decisions, however, on RIPE policies are not made during the RIPE meetings. Policy-making decisions are made only through the mailing lists. Therefore, the least precondition for participation in the discussions and policy-making process of the RIPE community is access to an email account, so one can subscribe to the mailing lists. No further requirements or obligations exist. This way the RIPE community allows all interested parties of the Internet community in this area to participate.

Furthermore, because the Internet has no geographic limits and because interconnection with networks in other geographic areas is a precondition for the proper functioning of the Internet, the participation of people from other regions is also encouraged in the policy development process. All in all, anyone with an interest in the development of RIPE policies is allowed and encouraged to participate so that RIPE policies are representative of all relevant stakeholders and reflect their actual needs and interests.

---

18. Blokzijl R., Lindqvist K., Yilmaz F., (2010), Policy development Process in RIPE, ripe-500, online at <http://www.ripe.net/ripe/docs/ripe-500>, accessed 18.04.2011.

19. More information about the RIPE Working Group mailing lists can be found online at <http://www.ripe.net/ripe/mail/wg-lists> / accessed 18.04.2011.

Consequently, the RIPE community has active participants from all geographic areas and all relevant sectors, both from the private and the public sector (industry, academia, government etc.). In other words, policy development within the RIPE community is done on a multistakeholder and multilateral basis and international co-operation.

### **Transparency**

In order for the RIPE community to make sure that the policy making process is not taking place “behind closed doors” and that all interested parties have sufficient information about the relevant discussions, it has been decided that all developments are transparent to everyone. Transparency is accomplished in the following ways:

- All developments are announced through the mailing lists.
- All discussions taking place through the mailing lists are archived in a comprehensive way and are publicly available.
- All discussions and developments that take place at the RIPE Meetings are webcast, recorded, archived and publicly available. In addition a transcript and the minutes of the discussions is archived and publicly available.
- All RIPE policies and announcements are archived and publicly available.

### **Bottom-up process**

The RIPE policy making process is designed so that anyone with an interest in participating knows how to participate and is able to do so. Anyone can propose a policy or an amendment of a current policy. Once a participant submits a policy proposal, other participants can submit their comments, support or objection to the proposal. This process adheres to established timeframes within which anyone can submit their feedback to the proposal but if the community needs more time to consider a particular proposal, these timeframes can be expanded.

The policies are created by the participants of the RIPE community. The individual participants of the RIPE community submit, comment on, and accept or reject a policy proposal. Should a proposal be accepted, the RIPE NCC has to implement it.

### **Consensus**

For a policy proposal to become a RIPE policy, consensus must be reached. All parties participating in the discussion must agree upon the proposal. There is no voting process since it is difficult to declare any kind of majority in an open forum with no defined membership such as the RIPE community. As a result if there are arguments or objection about a proposal, this proposal is not adopted.

### 3. Policies regulating the distribution of IP addresses

#### 3.1 *Principles for the distribution of IP addresses*

The RIPE community defines the criteria according to which IP addresses are distributed to networks in the RIPE NCC service region. These criteria are based on certain principles that were identified in 1996<sup>20</sup> and are acknowledged by the whole Internet community. These principles as articulated by the RIPE community are the following:

- Uniqueness
- Aggregation
- Conservation
- Registration

These principles are explained in the following paragraphs.

#### **Uniqueness**

For the proper functioning of the Internet Protocol, the IP addresses in an interconnected network must be unique, ensuring that devices on this network can be uniquely identified.

#### **Aggregation**

For technical reasons, routing a block of IP addresses that consist of numbers next to each other is more efficient and therefore preferable by the network administrators. For example, a network would more efficiently route 256 IP addresses consisting of the numbers 195.0.0.0 to 195.0.0.255 than 256 IP addresses consisting of numbers that are not contiguous.

Therefore, to ensure the proper operation of Internet routing, IP addresses must be distributed to networks in blocks of contiguous IPv4 addresses. Networks must be able to route the IP addresses allocated to them in a collective way.

#### **Conservation**

As the Internet grew and its application moved beyond research purposes, operators of Internet networks realized that the need of IP addresses would exceed the

---

20. See above, Hubbard K., Kusters M., Conrad D., Karrenberg D., Postel J., (1996), Internet registry IP allocation guidelines, RFC 2050.

number of possible IPv4 addresses. Therefore, IP addresses had to be allocated with “thoughtful care”.<sup>21</sup>

In 1996, the need for careful allocation of IP addresses was reflected in the principle of conservation of IP addresses. In order for the Internet registries to comply with this principle they had to distribute IP addresses fairly and according to the operational needs of the network the IP addresses would be allocated to. The prevention of stockpiling in order to maximize the lifetime of the IP addresses was highlighted.<sup>22</sup>

Accordingly, the RIPE community identified “conservation” as a goal of the Internet registry system. In particular, according to the IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region “Public IPv4 address space must be fairly distributed to the End Users operating networks. To maximise the lifetime of the public IPv4 address space, addresses must be distributed according to need and stockpiling must be prevented”.<sup>23</sup>

## Registration

The need to record in a public registry the IP addresses allocated to networks was identified from the early years of the Internet and became a principle for the RIPE community’s policies. This goal has two aspects: the insurance of uniqueness of the IP addresses distributed and the provision of contact information of networks for Internet troubleshooting at all levels.<sup>24</sup>

### 3.2 Can IP addresses be owned?

In the everyday language network operators use a wording that creates the impression that IP addresses are “owned” by them. The question is consequently whether IP addresses could be considered as a property that can be owned or sold by the organisations they are registered to.

To reply to this question, one should consider the principles and goals according to which IP addresses are allocated. According to the conservation principle all IP

---

21. See above, Cerf V., (1990), IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet «Connected», RFC 1174.

22. See above, Hubbard K., Kusters M., Conrad D., Karrenberg D., Postel J., (1996), Internet registry IP allocation guidelines, RFC 2050.

23. Bush R., Carr B., Karrenberg D., O'Reilly N., Sury O., Titley N., Yilmaz F., Wijte I., (2011), IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region, ripe-509, online at <http://www.ripe.net/ripe/docs/ripe-509> / accessed 18.04.2011.

24. See above, Hubbard K., Kusters M., Conrad D., Karrenberg D., Postel J., (1996), Internet registry IP allocation guidelines, RFC 2050.

address allocations and registrations are based on need. This principle is reflected in the procedures that are followed before and after IP addresses are allocated.

Before the allocation of the IP addresses, the requiring organisation must demonstrate a justified need for the allocation of IP addresses. If an organisation does not operate a network that is meant to interact with other networks in the Internet, the RIPE NCC will not allocate IP addresses to them. Apart from that the organisation must justify the number of IP addresses it requests. The RIPE NCC will allocate as many IP addresses as are needed by the set up of the relevant network, the number of the devices within the network etc, regardless of the number of IP addresses an organisation is requesting.

After allocation, the IP addresses remain under the control of the Regional Internet Registries. Local Internet Registries must adhere to the policies of the Regional Internet Registries and it is the responsibility of the Local Internet Registries to make sure that their customers follow the same policies. Additionally, all IP address allocations are subject to audits and verification controls as specified by the assigning Regional Internet Registry. If the network no longer meets the original allocation criteria or the allocation was based on false information, the registry will deregister the IP addresses and will make them available for a new, valid allocation.

Further, organisations are not entitled to transfer allocated IP addresses to a different organisation unless such a transfer is approved by the Regional Internet Registry. For such a transfer to be approved by the Regional Internet Registry, the acquiring party must meet the same criteria that would apply to them if they were requesting IP addresses from the Regional Internet Registry.

Finally, organisations that do not comply with these policies, lose their rights to the registration of the IP addresses.<sup>25</sup>

In conclusion, the allocated IP addresses are not property of the organisation they are allocated to.

---

25. See above, Hubbard K., Kosters M., Conrad D., Karrenberg D., Postel J., (1996), Internet registry IP allocation guidelines, RFC 2050, Bush R., Carr B., Karrenberg D., O'Reilly N., Sury O., Titley N., Yilmaz F., Wijte I., (2011), IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region, ripe-509 and RIPE NCC, Closure of LIRs and Deregistration of Internet Number Resources, ripe-517, online at <http://www.ripe.net/ripe/docs/ripe-517> / accessed 18.04.2011.

### 3.3 Public registry – the RIPE Database (whois)

#### 3.3.1 The purpose of the RIPE Database

Along with the need to keep records of the distributed IP addresses in an organised manner, network operators realised also the need to “know each other”, to determine the use of particular ranges of IP addresses by particular networks and to communicate with operators of other networks. Based on this information, they would also be able to peer with each other for routing purposes and enhance the efficiency of Internet traffic.

This information should be collected in one database and remain publicly available in an organised manner. This task was delegated to the Regional Internet Registries. The RIPE NCC implemented this mandate by creating the RIPE Database, which is also known as a “whois database”.

Information publicly available in the RIPE Database can be divided into the following categories:

- Information about organisations (usually LIRs), to which IP addresses are allocated by the RIPE NCC. This includes the name of the organisation as well as some technical contact details of natural persons responsible for managing technical problems with regards to the allocation that can be reported by third parties. The RIPE NCC is responsible for collecting this information and making it publicly available.<sup>26</sup>
- Information about networks or customers to which IP addresses have been assigned by LIRs. This is necessary for two reasons: first, to provide operational information about the use of the network and contact details in case of operational/security problems; and second to ensure that LIRs have indeed exhausted a majority of their allocation and therefore can justify receiving an additional allocation.<sup>27</sup>
- Routing information: The RIPE Database has information necessary to permit network administrators to make decisions as to the acceptability of traffic coming from and going to different legitimately allocated IP addresses.<sup>28</sup>

---

26. See above, Blokzijl R., Devillers Y., Karrenberg D., Volk R., (1990), RIPE Network Coordination Center (RIPE NCC), ripe-19.

27. See above, Hubbard K., Kusters M., Conrad D., Karrenberg D., Postel J., (1996), Internet registry IP allocation guidelines, RFC 2050.

28. See above, Cerf V., (1990), IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet «Connected», RFC 1174.



### 3.3.2 Quality of the RIPE database

It is very important that data collected in the RIPE database is accurate, correct and up-to-date. It is the responsibility of LIRs to provide the registry with correct and updated information. LIRs are also obliged to comply with audit controls performed by the RIPE NCC, for the purposes of assessing the data quality of this information.<sup>29</sup> The RIPE NCC also ensures the quality of this data everytime the LIR asks for an additional allocation.<sup>30</sup>

### 3.3.3 Data protection aspects

The registration of personal contact details in the RIPE Database does not refer to the registration of the actual user of a specific device connected to the Internet. It refers to the registration of the organisation (for example, the ISP) that is responsible for the maintenance of the network that corresponds to a block of IP addresses.

To facilitate communication among persons responsible for networks in case of a technical disorder, every registered organisation is obliged to provide and to keep updated the professional contact details of persons that, because of their profession, are responsible for the administration and the technical maintenance of each network. These contact details are very important for the smooth and uninterrupted operation of Internet connectivity. It should be stressed once again that these persons have nothing to do with the actual users of devices.<sup>31</sup>

To avoid this misunderstanding the RIPE NCC does not use the term “whois” when referring to their public database, but refers to the RIPE Database.

## 4. Challenges

### 4.1 *The run out of IPv4 addresses*

Although IPv4 addresses were numerous enough for the needs of the 1980s, later on the unpredicted success of the Internet later on meant that they were insuffi-

---

29. RIPE Database Terms and Conditions, online at <http://www.ripe.net/data-tools/support/documentation/terms> / accessed 18.04.2011.

30. See above, Hubbard K., Kusters M., Conrad D., Karrenberg D., Postel J., (1996), Internet registry IP allocation guidelines, RFC 2050, Blokzijl R., Devillers Y., Karrenberg D., Volk R., (1990), RIPE Network Coordination Center (RIPE NCC), Bush R., Carr B., Karrenberg D., O'Reilly N., Sury O., Titley N., Yilmaz F., Wijte I., (2011), IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region, ripe-509.

31. RIPE NCC Privacy Statement, online at <http://www.ripe.net/lir-services/ncc/legal/ripe-ncc-privacy-statement> / accessed 18.04.2011.

cient. The careful allocation of the IPv4 addresses based on demonstrated need for the purposes of the conservation of the IP addresses or other “tricks”, such as the use of “dynamic” IP addresses by Internet Service Providers could only postpone the inevitable run out of IPv4 addresses.

In the beginning of 2011, more than 95% of the IPv4 addresses have been allocated, assigned or otherwise reserved. The IANA free pool of IPv4 address was exhausted in February 2011. Many of the addresses are with the five Regional Internet Registries or have been allocated by them.

The RIPE community, realising the need for a fair distribution of the last IP addresses and taking into account the need of future/not-yet-existing LIRs to have access to IPv4 addresses to manage the transition to IPv6, has come up with a policy according to which only small blocks of the last IPv4 addresses would be distributed to LIRs that have already been allocated IPv6 addresses<sup>32</sup>. Taking into account that IPv6 addresses are allocated only if there is a plan for IPv6 infrastructure, the RIPE community also tried with this policy to give LIRs an incentive to deploy IPv6; either an LIR has to plan to deploy IPv6 or it does not receive a share of the last IPv4 addresses.

#### ***4.2 Maintaining a good registry***

After the depletion of the IPv4 addresses, distribution of IP addresses will no longer be the main function of the Regional Internet Registries. IPv6 addresses are not allocated in the same way as IPv4. For technical reasons IPv6 addresses cannot be allocated individually to End Users but as subnets. A single user of a computer is generally entitled to be assigned  $2^{64}$  addresses.

Therefore Regional Internet Registries are focusing on maintaining the registration of IP addresses, which is still a very important activity for the operation of the Internet. Maintaining an up-to-date registry will be the primary goal of the Regional Internet Registries. Information about the networks to which IP addresses have been distributed is and will continue to be controlled. However, this goal faces the following challenges:

- A request for an additional IPv4 address allocation by the RIPE NCC was an opportunity for the performance of an audit by the RIPE NCC regarding the quality of their registration data of the LIR. Now with the large blocks of IPv6 addresses that are distributed to LIRs, requesting an additional allocation is not foreseeable.

---

32. Smith P., Bidron A., (2011), Allocations from the last /8, 2010-02, online at <http://www.ripe.net/ripe/policies/proposals/2010-02>, accessed 18.04.2011, see above Bush R., Carr B., Karrenberg D., O'Reilly N., Sury O., Titley N., Yilmaz F., Wijte I., (2011), IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region, ripe-509.

The obligation to keep the records in the publicly available database correct and up-to-date is no longer easy to enforce.

- Although after the creation of the RIR system the allocation of IP addresses adhered to a concrete system that was defined by certain principles, policies and contractual obligations, quite a few addresses were given out before the formation of the RIR system. As much as IP addresses distributed by the RIPE NCC are registered and maintained in the RIPE Database, IP addresses distributed in the early years of the Internet (known as “legacy space”) constitute a large number of addresses that are neither properly registered nor clearly adhere to the RIPE policies. The RIPE NCC and other RIRs are now trying to collect all possible information about these IP addresses and update their records in their registries because after the depletion of IPv4 addresses, the possibilities of hijacking unregistered and unconfirmed addresses is very high. However the RIRs depend on the holders of these IP addresses to cooperate with these efforts and to comply in the future to Internet community policies.

#### ***4.3 Commercialisation of IPv4 addresses***

Although the need for more IP addresses was identified in the 1990s, implementation of this new protocol has not yet been achieved. Currently 66% of the LIRs in the RIPE NCC service region have not requested IPv6 addresses.

The exhaustion of IPv4 addresses in combination with the unwillingness of the industry to implement IPv6 addresses will lead to a situation where IPv4 addresses become extremely valuable and their use extremely complex. ISPs or other LIRs or users attach value to IP addresses by applying property features to them, e.g. by commercialising (selling) them or by treating them as assets.

Discussions are currently taking place around the designation of IPv4 addresses as “public resources” and the proper and fair allocation of unused IPv4 addresses in light of this.<sup>33</sup> However while IPv4 addresses are indeed scarce resources and their distribution must be fair, the question is whether it is appropriate to investigate methods of reallocating when IPv4 addresses cannot meet the demands of the Internet in the long run.

This issue would be solved with the deployment of the IPv6 protocol. But the high investment that this deployment requires and the lack of incentives by the public and the private sector create obstacles to the solution of the problem.

---

33. Weber R. H., Heinrich U. I., IP Address Allocation through the Lenses of Public Goods and Scarce Resources Theories (2011), online at <http://www.law.ed.ac.uk/ahrc/script-ed/vol8-1/weber.asp> / accessed 18.04.2011.

# The EU Data Protection Directive revised: new challenges and perspectives

---

---

Maria Giannakaki

---

---

## I. Introduction

Our society undergoes fundamental changes due to the rapid technological developments and globalization that have given rise to the processing of data on a worldwide scale and an increase in international cross-border data transfers. The expansion of social networking services (SNS) and the growing demand for cloud based services (IaaS, Paas, SaaS) trigger new perspectives, but also new practical data protection challenges.

Although it is accepted that widely applauded principles of the EU Data Protection Directive 95/46/EC for the protection of personal data still remain valid, it is equally acknowledged that the existing EU legal framework needs to be revised in order to cope with the evolutions.

To that end on November 4, 2010 the European Commission released a Communication proposing ‘a comprehensive approach on personal data protection in the European Union’ with a view to amend the EU Data Protection Directive 95/46/EC (“the EU Directive”).<sup>1</sup> The Communication is the result of the review of the current legal framework, which started with a high-level conference in Brussels in May 2009 and was followed by a public consultation during 2009 and 2010.<sup>2</sup> On February 2011, the Council of the European Union released its conclusions on the Communication and outlines the main axes of the reform.<sup>3</sup>

- 
1. European Commission (2010), Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions “A comprehensive approach on personal data protection in the European Union” on line at [http://ec.europa.eu/justice/news/consulting\\_public/0006/com\\_2010\\_609\\_en.pdf](http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf) / accessed 01.04.2011.
  2. Article 29 Data Protection Working Party (WP29), The Future of Privacy, 01.12.2009 [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf) accessed 24.03.2011.
  3. Councils Conclusions on the Communication from the Commission to the European Parliament and the Council – A comprehensive approach on personal data protection in the European Union (2011) on line at [http://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/jha/119461.pdf](http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf) / accessed 02.04.2011.

This paper aims to analyze the data protection challenges under new technological and social developments, examine how the current data protection rules address these issues and identify the possible solutions in light of the current reviewing process of the EU Directive.

## II. Challenges: Technical and social developments

### II.1. Utility computing – The ‘cloud’

In recent years, cloud computing has emerged as one of the fastest-growing segments of the information technology industry. According to the European Network and Information Security Agency (‘ENISA’), the worldwide forecast for cloud services in 2013 amounts to USD 44.2bn, with the European Market expected to go from € 971 in 2008 to € 6005 in 2013.<sup>4</sup>

Cloud computing “is an on-demand service model for IT provision, often based on visualization and distributed computing technologies”<sup>5</sup>. It is an internet-based model of computing enabling the provision of various services upon demand, such as Infrastructure “IaaS” (e.g. compute power, storage, servers and related tools, such as Windows Live Skydrive and Rackspace Cloud), Software “SaaS” (e.g. software applications deployed as a hosted service and accessed over the internet via a standard web browser such as Zoho.com, Google docs) and/or Platform “PaaS” (e.g. operating systems and associated services over the Internet without downloads or installation such as Google App Engine)<sup>6</sup>. For the provision of such services, Cloud Service Providers (“CSP”) are based on “a networked collection of servers’ storage systems and devices combining software, data and computing power scattered in multiple locations across the network.”<sup>7</sup>

Cloud computing offers several benefits for both users and service providers, such as services provided on demand without the need for certain software or hardware at the physical point of access, cost savings, easy access and implemen-

---

4. European Network and Information Security Agency (ENISA), 2009, “Cloud Computing: Benefits, risks and recommendations for information security”, online at [www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing.../fullReport/](http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing.../fullReport/) accessed 24.03.2011.

5. Id. no 4.

6. Joep Ruiter and Martijn Warnier (2011), “Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice”, online at <http://homepage.tudelft.nl/68x7e/Papers/spcc10.pdf> / accessed 03.04.11.

7. Ann Cavoukian, Information and Privacy Commissioner of Ontario, (2008), “Privacy in the clouds: A White Paper on Privacy and Digital Identity: Implications for the Internet”, online at <http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf> / accessed 24.03.2011.

tation by small and medium enterprises (SMEs) etc.<sup>8</sup> Arguably, “the cloud” is turning computing into a utility due to the fact that it enables the packaging of computing resources, such as computation, storage and service and makes them available on demand in a way similar to the traditional public utility (such as electricity, water, natural gas or telephone network).<sup>9</sup>

However, due to its ubiquitous and dynamic nature cloud computing also raises serious concerns from a data protection and privacy perspective. In the “cloud” the CSPs’ servers are located in several jurisdictions, data is processed and ‘duplicated’ in a variety of locations around the world and transferred from one location to another and infrastructure used to store and process a customer’s data is shared with other customers. Data processing “in the cloud” involves outsourcing partial control over the storage, processing and transmission of such data to a CPS due to the fact that the CPS determines the location of data, the service and the security standards.

On 03.02.2011 the Danish Data Protection Authority issued a Resolution (0138-52-2010), rejecting the Municipality of Odense’s planned use of Google’s Cloud Computing services within schools over cloud privacy risks.<sup>10</sup> Last year the German Data Protection Authority issued a Framework Paper and an Opinion addressing the various legal concerns regarding personal data protection and data transfer in the cloud, with the aim to impose tougher restrictions and requirements to cloud computing and other outsourcing arrangements involving personal data.<sup>11</sup>

---

8. Sneha Prabha Chandran and Mridula Angepat, “Cloud computing: Analysing the risks involved in cloud computing environments” online at [http://www.idt.mdh.se/kurser/ct3340/ht10/FinalPapers/16-Sneha\\_Mridula.pdf](http://www.idt.mdh.se/kurser/ct3340/ht10/FinalPapers/16-Sneha_Mridula.pdf) / accessed 03.04.11.

9. Nicolas Carr, (2008), “*The Big Switch – Rewiring the world from Edison to Google*”, W.W. Norton.

10. The Municipality planned to use Google Apps in order to allow teachers to register among others information about lesson planning and student’s educational developments. The Authority expressed concerns about the security of sensitive data, the transfer of data to other countries, deletion of data, use of encryption and whether the data is logged and for how long the log is stored. Decision of the Danish Data Protection Agency on the use of cloud computing services within schools online at <http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/> /accessed 01.04.11.

11. German Data Protection Authority, (2010) “*Legal Opinion on cloud computing*” online at <https://www.datenschutzzentrum.de/cloud-computing> & “*Draft Framework Paper on cloud computing*” online at [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Sonstige/Cloud\\_Computing\\_Mindestsicherheitsanforderungen.pdf?\\_\\_blob=publicationFile#download=1](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Sonstige/Cloud_Computing_Mindestsicherheitsanforderungen.pdf?__blob=publicationFile#download=1) / accessed 24.03.2011.

Cloud computing triggers several legal issues from a data protection point of view which can be summarized as following:

### **1.1 Applicable law in the cloud: Territoriality v. country of origin principle**

Under the EU Data Protection Directive (art. 4), “each member state shall apply the national provisions it adopts pursuant this Directive to the processing of personal data where: a. the processing is carried out in the context of the activities of an establishment of the controller on the Territory of the Member State or in a place where its national law applies by virtue of international public law or b. the controller is not established on Community territory and for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said member unless such equipment is used only for purposes of transit through the territory of the community.”

Under the current provisions of the Directive, the starting point of the applicability criteria is the place of establishment of the organization making decisions about the use of data or the use of equipment situated in the territory. Preamble 19 of the Directive clarifies that “establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements and when a single controller is established on the territory of several member states, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities”.

“In the cloud” the physical location and the use of means are no longer suitable connecting factors, as data effortlessly flows around the globe, ignoring boundaries and territories, and replicas of users’ data are kept in several multiple data centers located at random places and jurisdictions. On top of that, cloud computing services usually involve a multitude of providers, who may process data by determining both the purposes and the means of data processing or may process data on the instructions of their client.

When applying the territoriality principle in cloud computing services, determining which cloud provider is subject to EU data protection rules for what data processing can prove to be a very difficult task. If a CSP is established in the EU and/or uses equipment in the EU, he will be subject to the EU data protection law. However, if he is not established in the EU and/or does not use equipment in the EU, he would not be subject to the European law, even if European citizens’ data are processed through cloud computing services.

## 1.2 Role distribution in the cloud: Data controller v. data processor

The question of applicable law is directly related to the entity which will be qualified as a “*data controller*”. Under article 1 par d and e of the EU Directive the “controller” is the person who alone or jointly with others determines both the “*purposes*” and “*means*” of processing, while the “*data processor*” is the person who processes personal data “*on behalf of the controller*”. The controller is primarily responsible for the compliance with data protection obligations and will also be held liable in case of breach.

With respect to cloud computing, the identification of the data controller can prove to be a very difficult task depending on the type of the cloud computing that is used and the technical set-up of the system. A CPS usually processes clients’ personal data “on their instructions” and for the purposes that they have determined. However, at the same time the CPS makes decisions at its sole discretion about the “means of data processing” regarding the location of the data, the service levels, security and the related technical and organizational measures.

Given that the concepts of the data controller and data processor are not clear<sup>12</sup> it would be rather difficult to identify on a case-by-case basis who is the data controller. It is also quite possible that the basic decision on who is responsible for data protection compliance would be contested. It is likely that CPS will consider themselves to be data processors in order to avoid step in the shoes of the data controller and bear the burden to comply with data protection obligations.

Consequently, the customers, who are very unlikely to know if and when their data are moved, how they are stored, who has access to them and which security measures have been put in place, will end up to be solely responsible for data protection compliance, except maybe from cases like platform as a service where a user does not have any control over the means used to process data or if the CPS analyses users’ personal data for the purposes of behavioral advertising.

## 1.3 Purpose of processing in the cloud: business v. purely personal purposes

There is a tendency to offer cloud computing services to individuals as end users, such as storage of pictures, calendars, typically the type of information one should keep at home and use for personal purposes. However, article 3 of the EU

---

12. WP 128, 22.09.2006 and WP 169, 16.02.2010 with regard to the determination of the means of processing and the criterion of the “essential elements of means” online at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128\\_el.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_el.pdf) and [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf) / accessed 24.03.2011. On the term “data controller” and civil liability, see Bottis M., *Civil liability for illegal processing of personal data*, Civil Law Applications, 2009, issue 7, pp. 784-797.



Directive excludes from its scope of application data processing carried out “by natural persons in the course of a purely personal or household activity (the “house hold exemption”).

Therefore, due to the personal – household nature of information uploaded to the cloud, processing activities that are carried out on behalf of the individuals involved may not fall under the scope of the EU Directive.

### **1.4 Transfers in the cloud: Jurisdictional approach v. international standards**

Cloud computing entails the continuous transfer of personal data. The EU Directive prohibits transfers of personal data outside EU/EEA and a limited number of “third countries” considered by the European Commission as providing “adequate safeguards”, based on the presumption that these countries do not always protect personal data sufficiently, unless the CPS provides adequate safeguards for such protection.

Although in theory a variety of possible legal bases for adequate safeguards exists, in the cloud context it is very difficult to implement. A business most likely would rely on data subjects’ consent, the “balance of interests” test or contract fulfillment.

Obtaining consent inevitably would be burdensome and in any case, raises significant legal issues in Europe, for the reason that the CPS will have to prove that such consent has been freely given and that it is specific, informed and freely revocable. With regard to the “balance of interests test”, it would be rather difficult for CSP to apply this test in an international environment, due to its vague and open-ended nature, as well as in the different approaches by each Member State. A third option would be to use the EU model clauses or Binding Corporate Rules, however, given the onerous obligations they entail and the fact that they are designed for multinational companies and do not always work well in a multi-tiered vendors relationship, this option may become problematic too.

## **II.2. Social computing - Web 2.0**

Cloud computing is an innovation in the technical way services are provided. However, nowadays there is also a significant social evolution in the way the Web is used to such extend that many speak about the creation of a new version of World Wide Web: Web 2.0.<sup>13</sup> Arguably, Web 2.0. presents a second generation of web-based communities, applications and hosted services that facilitate par-

---

13. O’ Reilly (2005), “What is Web 2.0” online at <http://facweb.cti.depaul.edu/jnowotarski/se425/What%20Is%20Web%202%20point%200.pdf> / accessed 01.04.2011.

ticipatory information sharing, interaction and collaboration on the World Wide Web. Examples of Web 2.0 include Social Networking Sites “SNS” (such as Facebook, Myspace, Twitter, LinkedIn), blogs, video sharing sites, hosted services, web applications and mash-ups.

## 2.1 Web 2.0 characteristics

Web 2.0 allows users to use “Web as a Platform” in order to create and distribute their own User Generated Content (“UGC”), promotes creativity, collaboration and sharing through mass social networking channels. Furthermore, it facilitates users to express themselves, engage in social and political debates, access and participate in economic, cultural and administrative activities, contribute to the production of knowledge and eventually construct their public profile. Social networking providers (SNP) serve as a tool enabling users to create and exchange content and communication and eventually promote the exercise and enjoyment of human rights and fundamental freedoms, in particular the freedom of expression.

However, the ubiquitous character of information in the Web 2.0 environment poses new challenges to the application and enforcement of data protection principles. Data from different locations and sources are collected, visualized and aggregated by Search Engines, Social Network Aggregators (Spokeo, Pipl)<sup>14</sup> and Mass-ups (Poplfly)<sup>15</sup> in applications that combine different types of information such as geolocalization data, photos, audio and other information and make them available into a single view.

Web 2.0 increases the accessibility to any kind of information related to individuals regardless if it refers to his private, public or professional life and makes it accessible to any internet user who is interested to perform a research about a persons’ virtual identity: human-resources professionals report that their companies require them to do on line research image tagging by third parties, many SNS and other providers of “free” cloud computing services (such as webmail) seize the opportunity to monetize users’ information by including targeted advertisements in their offerings. Soon Web 2.0 will be used as a platform by which people will be rated, assessed and scored not only on their creditworthiness, but also on their reputation and trustworthiness as good parents, dates, employees, insurance risks etc.

---

14. Social Network Aggregators are web sites that aggregate data publicly available from on-line and offline sources (such as phone directories, social networks, photo albums, market surveys, mailing lists and business sites) and permit username search scan across the web constructing online profiles on real time.

15. Mash-up is a web-application based technology that uses and combines multiple web sources and creates a new service enabling users to have access to different types of media such as data, video, images, blogs and audio into a single view.

Also, information is copied, tagged, reposted and remains in search engines, aggregators, mass-ups and internet archives for an indefinite period. Technology enables users to retrieve in a matter of seconds' information which would otherwise be forgotten – and 'forgiven'. According to ENISA, Internet in the Web 2.0 era has the "Hotel California impact" on individuals: "*They can check out any time they like but they can never leave*"<sup>16</sup>.

## 2.2 Data subjects' rights under the current legal framework

The above characteristics of social computing, result to a loss of control over individuals own data, due to the fact that it is practically impossible to know what data are being collected, how they are processed on what context they are used and for what purpose and if they are secure. Information is '*alienated*' from the individual and the context in which it has been initially disclosed.<sup>17</sup>

Under the current EU data protection framework, the constitutional right to informational self-determination<sup>18</sup> warrants the capacity of individuals to determine in principle the disclosure and use of their personal data and decide what information about themselves should be communicated and under what circumstances. In addition to that, the EU data protection Directive provides for data subjects' right to access and/or rectify their personal data, withdraw their consent for data collection and processing or delete them.

Furthermore data controllers bear the obligation to keep data collected for a specific retention period which is related to the scope of their processing and in any case they should keep data no longer than necessary. Given that this specific period lapses, they should delete them in order to satisfy data subjects need to "be forgotten".

However, Web 2.0 platforms make the application and enforcement of these rights extremely difficult. In an attempt to strengthen data subjects' rights and help them ensure control over their data, the "*right to be forgotten*" is proposed to be inserted in the revised EU Directive. This right has since been implemented in Europe.

---

16. ENISA "Security issues and Recommendations for Online Social Networks" (2007), online at <http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks/> accessed 04.04.2011.

17. Lilian Mitrou, "Privacy in Web 2.0" (2010), DiMMEE, 3/2010, page 323 (in Greek).

18. Ruling of the German Constitutional Court defining informational self-determination online at <http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm> /accessed 23.03.2011.

### III. Perspectives – Key issues for amendment

The aforementioned challenges of the new technological and social developments are addressed among others in the ongoing procedure of amendment of the EU Directive.

#### *III.1. International dimension of data protection*

##### **1.1 Applicable law**

Under the current provisions of the EU Directive, it is not always clear to both data controllers and data protection supervisory authorities which member state is responsible and which law is applicable when several member states are concerned. It is therefore commonly agreed that there is a need to enhance legal certainty and avoid potential conflicts between overlapping data protection laws. More specifically, the Council concluded that *“the new legal framework should clearly regulate the issue of applicable law within the EU in such a way so as to allow data subjects to effectively exercise their rights and to provide legal certainty to data controllers in cross-border activities.”*

To that end, it seems that all parties<sup>19</sup> agree that privacy standards for EU citizens should apply independently of the area of the world in which their data is being processed and that the national privacy authorities should be endowed with powers to investigate and engage in legal proceedings against non-EU data controllers whose services target EU consumers, such as US based social network companies which have millions of active users in Europe or cookies from non-EU sites.

More specifically, the criteria for determining applicable law should change from establishment and equipment to citizenship or residency. The country of origin principle is presented as a better, clearer and unambiguous rule on applicable law, which shall enable each Member State's law to apply to the state citizens or residents in the same way as for example the US Federal Trade Commission standards apply with respect to enforcement of the Children's Online Privacy Protection Act, in case that US children are targeted by a service provider.

However, it has been identified<sup>20</sup> that harmonization or at least approximation at a high level between the laws of the member states is an essential prerequisite in order to avoid “forum shopping”.

---

19. European Commission, European Council, WP29, the EU Commissioner for Justice, Fundamental Rights and Citizenship, the European Data Protection Supervisor and participants in the public consultation.

20. European Commission – DG JFS, New Challenges to Data Protection – Final Report [http://ec.europa.eu/justice/policies/privacy/docs/studies/new\\_privacy\\_challenges/fi-](http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/fi-)

The concept of “targeted individuals” or the “service orientated approach” is also followed by the EU Regulation 593/2008 on the law applicable to contractual obligations (Rome I), which provides that the absence of a valid choice of law a consumer contract “shall be governed by the law of the country where the consumer has his habitual residence provided that the professional: a. pursues his commercial or professional activities in the country where the consumer has his habitual residence or b. by any means, directs such activities to the country or to several countries including that country”. Further guidance with regard to the criteria of “directed activity” can also be found in Recital 24 of Rome I.”<sup>21</sup>

## 1.2 Harmonization within the EU/EEA countries

The Council recognizes that the most important element of a well-harmonized approach in Member States is a new legal framework providing for a higher level of harmonization than the current one, without specifying the legal instrument by which this harmonization could be achieved.

There are various suggestions as to how this purpose of harmonization can be achieved: The European Data Protection Supervisor advocated for a regulation rather than a Directive for the reason that if the new legislation takes on the form of a Regulation, it would be directly applicable to all member states under the EU law, without the need for a separate implementation into national law, as would be the case for a “Directive” and that would considerably facilitate the global transfer of data outside the EEA.<sup>22</sup>

Regardless the above proposal, it is widely accepted that there will be no need to amend the Directive or to insert a Regulation but give the power to the WP29 to carry out more in-depth, surveys of national laws and practice with the view to formulate best practices and suggested interpretations.<sup>23</sup>

## 1.3 Simplification of International Data Transfers

With regard to the International Data Transfers, the challenge would be to find a model that achieves in practice without imposing disproportionate burdens on

---

nal\_report\_en.pdf / accessed 31.03.2011.

21. Lokke Moerel (2011), “The long arm of the data protection law”, International Data Privacy Law, 2011, Vol 1, N01, online at <http://idpl.oxfordjournals.org/content/1/1/28.full.pdf+html>/ accessed 05.04.11.

22. Opinion of the European Data Protection Supervisor on the Communication from the Commission (2011) online at [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14\\_Personal\\_Data\\_Protection\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf)/ accessed 31.03.2011.

23. Id. no 20.

organisations, economic development or innovation of multinational companies in particular.

To that end, the Commission intends to improve and streamline the current procedures for international data transfers, including legal binding instruments and BCRs in order to ensure a more uniform and coherent EU approach vis-à-vis third countries and international organisations.

This goal can be achieved by a greater recognition of adequacy of non EU/EEA companies, as well as a review of the BCRs as a legal basis for data transfer. In addition to the above, the Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data presented to the 31<sup>st</sup> Conference of Data Protection and Privacy Commissioners would also provide valuable assistance.<sup>24</sup>

### **III.2. Individuals' rights**

#### **2.1 Right to be forgotten and data portability**

The Commission in its Communication announced that it wishes to find ways to clarify the "*right to be forgotten*", the right of individuals to have their data deleted when they are no longer needed for legitimate purposes especially in cases that processing is based on the person's consent which is withdrawn or when the storage period has expired. The right to be forgotten will complement the existing rights of data subjects by ensuring data portability: the explicit right for an individual to withdraw his/her data.

The Council encouraged the Commission to explore the introduction of a "*right to be forgotten*" as an innovative legal instrument, even though the exact content of such right and the conditions on which it will be exercised has not been defined yet.

The "*right to be forgotten*" is not a new concept. The right to oblivion (*droit à l'oubli*) is a right related to data subject's right to withdraw their consent for data processing and have their data deleted<sup>25 26</sup> and is directly related to the right to informational self-determination.

---

24. Data Protection and Privacy Commissioners "*Joint Proposal for setting International Standards on Privacy and Personal Data Protection*" (2011) [http://www.privacyconference2009.org/dpas\\_space/Resolucion/common/resolution\\_international\\_standards\\_en.pdf](http://www.privacyconference2009.org/dpas_space/Resolucion/common/resolution_international_standards_en.pdf) / accessed 31.03.2011.

25. Lilian Mitrou, "Privacy in Web 2.0" (2010), DiMMEE, 3/2010, page 319 (in Greek).

26. Premier Ministre de la République Française, 2010, Charte «Droit à l'oubli dans les sites collaboratifs et les moteurs de recherche», [http://www.aidh.org/Actualite/Act\\_2010/](http://www.aidh.org/Actualite/Act_2010/)

According to the European Data Protection Supervisor, the “*right to be forgotten*” would ensure the deletion of personal data or the prohibition to further use them without necessary action of the data subject under condition that such data has already been stored for a certain amount of time. To that end, data will be attributed to some sort of expiration date.<sup>27</sup> Furthermore, the EU Commissioner for Justice Fundamental Rights and Citizenship clarified that data subjects and especially consumers will have the right and not the possibility to withdraw their consent to data processing and ask for the deletion of data being held on them, under condition that they prove that the collecting of their data is no longer necessary.

The “*right to be forgotten*” has been strongly criticized and has given rise to serious concerns regarding its achievability in the new technological and social environment, which can be summarized as following:

The exact content and scope of the right has not been clarified yet, obviously due to the fact that it would be rather difficult to determine what kind of records/information will be covered by such right (e.g. what is it to be deleted? the entire record? copies of records sent to third parties? archived copies?), who will be entitled to such right (when records e.g. are associated with multiple individuals), who will be subject to it and what would be the duties to be imposed (e.g. what would be the duty of a blog service in the context of an anonymous speech, where it would be unable to contact the creator of the record to be deleted).

The new powers that the new right actually entails are not clear. The right is implicitly established in the EU Directive, with the principle of data retention and the existing duty to keep data no longer than necessary in relation to the scope of their collection and data subject’s rights to access, rectify or delete data.

Such right should be carefully expressed in order to provide for counterbalancing exemptions where there is a need to preserve data irrespective of the individuals’ wishes e.g. for journalistic, literary and artistic purposes, freedom of expression, freedom of press, freedom of society to record history etc. Striking the appropriate balance between an individual’s “*right to be forgotten*” and other individual or societal interests such as the freedom of expression and the freedom of the press would be rather difficult and situations where the deletion is impossible, infeasible or socially harmful should also be addressed under the revised EU Directive.

---

Images/Charte\_oubli\_La\_Charte.pdf and <http://www.village-justice.com/articles/Internet-droit-oubli-numerique,9772.html> / accessed 31.03.2011.

27. European Data Protection Supervisor, Opinion on the Communication from the Commission to the European Parliament, the Council the Economic and Social Committee of the Regions [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14\\_Personal\\_Data\\_Protection\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf), accessed 29.03.2011.

The “*right to be forgotten*” has raised serious objections due to the fear that such a right may end up as a tool for censorship or the suppression of civil liberties in order to create a digital identity including only good information. There is a fear that it is rather possible that users may invoke libel or defamation in order to justify censorship about things that hurt their reputations.

The application of this right becomes much more complicated when related to the Web 2.0. platform providers, due to the fact that data to be deleted refer to the user’s content rather than the platform’s traffic data, as it might have been the case with the debate relating to cookies, logs data retention and e-discovery. For example, when data are published on an SNS, they are practically published to the whole Internet. The SNS may be able to offer deletion only in its own environment but not to other environments (such as search engines).

When it comes to search engines, mash-ups or social network aggregators things may become much more complicated with regard to the rights applicability: It is not obvious who will have the right to decide the data deletion in such cases. The SNS provider will be held responsible once the source of information is deleted from its site, to make sure that all reference to such information on the Internet is deleted? How can SNS delete information not included in their sites?

In addition to the practical and technical problems related to the deletion of information appearing in various different platforms on the Internet, there is also the issue related on the criteria on which platform providers will decide that data should be deleted or not. Who will be competent to decide whether the nature of information is defamatory or violates one’s privacy? Such control would oppose to the principle that intermediaries do not bear responsibility for the content, unless they are informed.

Two recent decisions of the Spanish Data Protection Authority and the Italian Courts prove that it is not going to be easy to strike the balance between the conflicting rights.

On January 2010, the Spanish Data Protection Authority accused Google of invading personal privacy of users, arguing that the company was in breach of the right to be forgotten. The Authority ordered Google to remove links to more than 80 news articles mentioning people by name saying it violated privacy for the reason that they contained out of date or inaccurate information. Google argued among others that this would be a form of censorship.

On April 2010, the Italian judge found Google criminally liable violating data protection law, in connection with the online posting of a video showing an autistic boy being bullied and insulted. More specifically, Google was found guilty for not taking precautions and not informing uploaders about their liabilities.



The Decision of the Italian Court has been strongly criticized for the reason that the Italian judge failed to conceptualize the role of platform providers in the concept of Web 2.0 and their enabling function with regard to User Generated Content. Establishing provider's liability for UGC would enable them to exercise a preventive and proactive control over the distribution of such content. This role is contrary to the current rules for limiting liability of host providers with regards to the contents published in their websites.<sup>28</sup>

On top of the above, the "*right to be forgotten*" would be rather difficult to apply in an international environment, given the different understandings of the notion of privacy. For example, in the US privacy is primarily related to consumers and it does not apply to any information in the public domain. The right to be forgotten has since the writing of this article been implemented in Europe (2012).

## 2.2 Alternatives

It is true that the web as a platform is a field of controversies and conflict of interests and it is questionable if the existing law may effectively address the various issues that arise. However, many think that the existing law deals with this well by permitting data retention as long as necessary and that hyper specific regulation will not work since the cases are simply too varied. Alternatively, the following amendments and measures may be put forward:

Data subjects should be better educated regarding the Web 2.0. so as their consent to be reinforced: "educated" data subjects may acknowledge that the UGC may jeopardize their private life. To that end, the Council supports the efforts of the Commission in drawing up EU standard privacy information notices, including the minimum set of information to be provided to data subjects and acknowledges the major need to increase the data subject's awareness of the implications of sharing his personal data.

Services should be better regulated in order to clarify the existing obligations and liability of the Web 2.0 providers on which ordinary users rely. In particular such hosts should be made to provide default settings for their sites and services and tools that are privacy friendly: If the default settings fail to protect privacy and personal data, the site that chose those settings should carry the primary responsibility for this. This would leave open the possibility of adopting a tort regime

---

28. Giovanni Sartor and Mario Viola de Azevedo Cunha, 2010, "The Italian Google-Case: Privacy, Freedom of Speech and Responsibility for Users-Generated Contents", *International Journal of Law and Information Technology* Vol. 18, No 4, Oxford University Press online at <http://ijlit.oxfordjournals.org/content/18/4/356.full.pdf/> accessed 05.04.2011 and Paul Mendez 2011, "Google Case in Italy" *International Data Privacy Law* online at [http://idpl.oxfordjournals.org/content/early/2011/02/25/idpl.ipr003.full /](http://idpl.oxfordjournals.org/content/early/2011/02/25/idpl.ipr003.full/) accessed 05.04.2011.

under which individuals can be held liable for wrongful or unjustified public disclosure of private information or intrusion over the Internet.<sup>29</sup>

In addition to the above, the existing duty to keep data no longer than necessary, should be further specified and clarified in relation to the specific activities for which data are collected. Data retention policies can be made compulsory and storage periods in data privacy notices can be further specified.

### 3. Proactive measures and self-co regulation

The EU Directive provides for *“the implementation of appropriate technical and organizational measures by the data controller aiming to protect personal data against accidental loss, alteration, unauthorized disclosure or access”*.

However, in practice it is widely accepted that the current notification process and relevant requirements are overly bureaucratic, achieve little real benefit and divert resources of controller and supervisory authorities away from substantial compliance work.

Under the current review of the EU Directive, it is acknowledged that the implementation of proactive measures though out the cycle of data's life can strongly complement law, as following:

#### 3.1 Principle of Accountability

On July 2010, the WP29 adopted an Opinion on the “Principle of Accountability”.<sup>30</sup> The WP recommended that a new principle should be introduced, which would require data controllers to put in place appropriate and effective measures to ensure compliance with the principles and obligations set out in the Directive. This principle is not new: article 17 (1) of the Directive requires data controllers to implement measures of both technical and organizational nature. However, these provisions have a limited scope. The Principle of Accountability would explicitly require data controllers not only to comply with the existing principles of the law, but also to put in place pro-active measures ensuring compliance (such as data protection policies, mapping procedures, privacy impact assessments etc), as well as retain adequate evidence in order to be able to demonstrate compliance to authorities upon request.

The WP29 encourages data protection in practice in a more scalable and flexible approach where *“controllers are required to take a strategic, risk based approach when*

---

29. Id. no 20.

30. Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability on line at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf)/ accessed 24.03.2011.

*determining effective and appropriate measures based on the nature of the personal information being processed and the risks represented by such processing”.*

The suitability of measures to be adopted should be decided on a case-by-case basis in light of the data controller’s specific circumstances and of the risks that may result from the data controllers intended data processing rather than requiring data controllers to adopt each and every measure on a predefined list.

Both the Commission and the Council welcomed the principle of accountability which should be explored with a view to diminish the administrative burden on data controllers for instance by simplifying or tailoring adequate notification requirements, including a uniform EU-wide registration form. The principle of accountability is seen as a practical means of ensuring the observance of data protection rules as well as helping data protection authorities in their supervision and enforcement tasks.

### 3.2 Privacy Impact Assessment

The UK Commissioner in its “Privacy Impact Assessment Handbook” encouraged both government and private entities to undertake assessments in order to assess and identify privacy concerns of a project and address them at an early stage. More specifically, *“Privacy Impact Assessment (PIA) is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIA help identify privacy risks, foresee problems and bring forward solutions”.*<sup>31</sup>

PIA constitute a form of pre-emptive compliance audit aiming at the identification and evaluation of the potential privacy implications of a system in order to address them at an early stage with a view to control, minimize or even eliminate the risks associated with the private life. It is agreed that PIAs play a vital role in achieving both privacy protection for individuals and risk management to private organizations and government entities, where in some jurisdictions have already become mandatory.<sup>32</sup>

The Council invited the Commission to explore the possibilities of promoting preliminary Impact Assessments however, only in relation to certain categories of data due to the high privacy risks they present, such as biometric data processed especially in the field of police and judicial cooperation in criminal matters.

---

31. Information Commissioner’s Office, 2009, “ICO PIA Handbook” on line at [http://www.ico.gov.uk/upload/documents/pia\\_handbook\\_html\\_v2/index.html](http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html) assessed 06.04.2011

32. Lilian Mitrou, “Privacy in Web 2.0” (2010), DiMMEE, 3/2010, page 319 (in Greek).

### 3.3 “Privacy by Design” Principle

In addition to the early privacy planning with PIA's, the Council invited the Commission to explore the possibility of including a provision on the “privacy by design principle” in the new legal framework related to the whole life-cycle of a system.

The principle of “Privacy by Design” was originally developed by the Ontario Privacy Commissioner according to which *“privacy and data protection are embedded through out the entire life cycle of technologies, from the early stage to their deployment, use and ultimate disposal”*. Recently, the 32<sup>nd</sup> International Conference of Data Protection and Privacy Commissioners issued a Resolution recognizing Privacy By Design as an essential component of fundamental privacy protection. According to the said Resolution, Privacy By Design is based on 7 foundational principals: i. Proactive not reactive, ii. Privacy by Default, iii. Privacy embedded into design, iv. Full functionality, v. Full lifecycle protection, vi. Visibility and transparency, vii. User centric.<sup>33</sup>

“Privacy by Design” also features in the Commission Communication on a “Digital Agenda for Europe – COM(2010) 245<sup>34</sup> by which it is acknowledged that it would empower data subjects to have more control over their personal data, through data minimization, privacy by default (default/initial settings should be protective for users privacy e.g. in social networks privacy by design would require to keep individuals profiles private by default and unavailable to search engines) and implementation of the necessary tools to enable users to limit the unnecessary collection of data and better protect their personal information (e.g. access controls encryption).

### 3.4 Private Enhancing Technologies (PETs)

The European Commission in its Communication to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), defines PETs as *‘a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or unde-*

---

33. Dr. Cavoukian, Information and Privacy Commissioner of Ontario, Canada, 2011, “Privacy by design resolution” on line at <http://www.ipc.on.ca/images/Resources/privacybydesign.pdf> accessed 06.04.11 and Data Protection and Privacy Commissioners – Resolution on Privacy by Design, Jerusalem, Israel, (27-29 October 2010), online at <http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf> /accessed 24.03.2011.

34. European Commission, 2010, “Agenda for Europe” on line at [http://ec.europa.eu/information\\_society/digital-agenda/documents/digital-agenda-communication-en.pdf](http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf) /accessed 06.04.11.

*sired processing of personal data, without losing the functionality of the Information System”.*<sup>35</sup>

PETs can be divided in two categories: PETs for privacy protection (PipeNet - protecting of identity when accessing interactive internet services, privacy technologies for RFID systems (out of tag mechanisms) and PET's for privacy management (such as eBay's Account Guard, Google's Safe Browsing toolbar)<sup>36</sup>.

They also include among others automatic anonymization after a certain lapse of time (e.g. anonymous credentials that prove an individual has permission to access specific resources without revealing its identity), encryption tools prevent hacking when the information is transmitted over the Internet (especially encryption for cloud Web services such as Google Docs to store and process data only in an encrypted form ensuring that access is limited to the owners of the data), “cookie-cutters” blocking cookies placed on the user's PC to make it perform certain instructions without being aware of them and Platform for Privacy Preferences (P3P) allowing Internet users to analyze the privacy policies of websites and compare them with the user's preferences as to the information he allows to release.

The Council invited the Commission to favor PETs as it is recognized that PETs are essential tools to ensure effective privacy protections however the challenge would now be to deploy these technologies in mass-market.

### 3.5 Personal data Breach Notification

The Breach Notification was inserted in the European law with the EU Directive 2009/136/EC (amending the E-Privacy Directive), which imposed notification requirements in case of a personal data breach (a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data) to competent authorities, subscribers and other affected individuals.

The insertion of a Data Breach Notification in the revised EU Directive could also serve as an effective remedy to individuals in order to be made aware of the risks

---

35. Communication from the Commission to the European Parliament and the Council on “*Promoting Data Protection by Privacy Enhancing Technologies (PETs)*”, (2007), on line <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:EN:PDF> accessed 10.04.11.

36. Final Report of London Economics to the European Commission DG Justice, Freedom and Security, about the study on the economic benefits of privacy-enhancing technologies, online at [http://ec.europa.eu/justice/policies/privacy/docs/studies/final\\_report\\_pets\\_16\\_07\\_10\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf) / accessed 06.04.2011.

they face when their personal data are compromised. In addition to the above, it could contribute to raise the awareness of data controllers in order to implement stronger security measures to prevent breaches and could also be used as a tool in order to enhance the principle of controllers' accountability.

The Council encouraged the Commission to explore the opportunity in extending data breach notification obligations to sectors other than the telecommunication sector. However, before implementing such obligation the costs to business and EU competitiveness should also be taken into account so as to avoid transforming the obligation to a routine alert for all sorts of security breaches. To that end, all stakeholders agree that the criteria for this selection should be the specific sectors in danger (such as the financial sector), the categories of events that may need to trigger notification, a risk assessment of the data breach, in order to avoid imposing cumbersome requirements.

### 3.6 Data Protection Officers and EU Certification Schemes

In addition to the above, the Commission underlined the fact that the current general obligation to notify all data processing operations to the Data Protection Authorities is a rather cumbersome obligation which does not provide, in itself any real added value for the protection of individuals' personal data.

Following, in the attempt to lessen the administrative and regulatory burdens to data controllers, the Council encouraged the Commission to include in its impact assessment an evaluation of the possible appointment of Data Protection Officers and supports the idea of introducing privacy seals (EU certification schemes) and self regulatory initiatives, by "*considering the establishment of a special body or office of the EU/EEA DPAs closely linked to the WP29 and the Commission to deal with the European Privacy Seal, European codes of Conduct and BCRs*".

The aforementioned schemes may provide comfort to users of certified technologies, however they should ensure that the criteria for granting such certifications are sufficiently technologically neutral and sufficiently flexible to take account of the fast pace of technological evolution.

## IV. Conclusion

The Commission will unveil legislative proposals to update the EU data protection legislative framework this summer.

Until now, it seems that the key issues for amendment would include the criteria on the applicable law, the harmonization of the internal market and the facilitation of international transfers. On the contrary, the proposed "*right to be forgotten*" has raised serious concerns by participants and stakeholders.

In addition to the above, even though it has been widely agreed that the roles of the different organizations have expanded far beyond the simple classification of the current EU Directive and are not properly covered by the confusing notions of data controller and data processor, the allocation of their responsibility does not seem to have been properly addressed during the consultation procedure.

On top of the proposed amendments, it is acknowledged that the sole law reform is not sufficient and there is a need for the adoption of preemptive “*quasi legal measures*” by the data controllers. It is acknowledged that it is going to be several years before any revised Data Protection Directive is agreed and in force throughout Europe. Therefore, in the meantime, organizations are encouraged to take the responsibility for their data privacy obligations through the adoption of data privacy compliance programs and in doing so they will hold themselves accountable to the stakeholders for the commitment to good practice.

# **A Web-based application for the registration of intellectual property**

---

---

**Andreas Giannakouloupoulos**

---

---

## **1. Introduction**

Scriptwriters Guild of Greece was founded in 1989. Its mission then as now is to protect writers' rights as creators and professionals in the audiovisual industry. As a constitutional member of the Federation of Scriptwriters in Europe (FSE), SGG helps the collaboration with fellow scriptwriters from other countries, caters for the protection of the rights of the scriptwriters, and impels the understanding of the importance of the script, in European and International level [SGG, 2011].

The Guild's main purpose is the promotion and protection of intellectual rights as well as of the creators' and writers' professional interests. Moreover, it solicits the designation, the exposure and the promotion of the scriptwriter's intellectual work which contributes to the creation of movies, television shows, radio programs, multimedia or any other audiovisual work. At the same time, one of the core priorities is to defend freedom of thought, speech and expression, as well as the development of collaboration with other Greek and international commissions that have either the same or similar goals.

The activities of SGG consist of giving seminars, participating in various committees and claiming the creators' rights by forcing the implementation of the relevant constitutional laws. Furthermore, it issues writings of cultural, artistic and professional content, offers consulting services to its members and has established special awards and honorary distinctions to scriptwriters and in general writers, both Greek and foreigners. Its members, successful and well-known creators, contribute to the amelioration of the artistic quality of the final product and the protection of the Greek language and the maintenance of the country's own specific national cultural identity.

Now the time has come for the Scriptwriters Guild of Greece to take a step forward. With the new web site [www.senariografoi.gr](http://www.senariografoi.gr) it opens new channels of communication, coming in direct contact with its members and with whoever is really interested in scriptwriting so as to help the Greek creators to bring forth their work and end the solidarity of the writing profession. Furthermore, through the new application that allows online registration, it assists writers and other



creators in establishing the completion dates of material written for films, television shows, radio programs and interactive media.

In order to better comprehend the need for such an application, this paper presents some historical evidence, economic aspects of intellectual property rights (IPR) and some international examples of similar projects. It also presents the useful results yielded during and after the process of developing this online application. These results refer to the difficulties and the technological restrictions needed to be considered in order this application to be complete in its function and successful in its legal role.

## 2. The setting

### 2.1 Brief history

Modern usage of the term “*intellectual property*” goes back to 1867 with the founding of the North German Confederation whose constitution granted legislative power over the protection of intellectual property to the confederation [Kawohl, 2008]. Twenty years later Victor Hugo and his comrades made the Berne Convention which took special pride in the establishment of the International Bureau which had administrative and educational responsibilities and the mandate to prepare for periodic revisions of the Convention [Oman and Flacks, 1993, p. 139]. The organization was subsequently relocated in Geneva in 1960 and was succeeded in 1967 by the World Intellectual Property Organization (WIPO) by treaty as an agency of the United Nations, created to monitor adherence to these conventions. In the generations that have followed, the United International Bureau for the protection of Intellectual Property (BIRPI) and WIPO have been active players in the development of international intellectual property laws.

In the 1980s there were already in existence multilateral agreements to protect IPRs and their most important goal was to create a set of enforceable international minimum standards. But the business networks and U.S. and European governments were dissatisfied with these agreements because they had low standards, did not have enforcement mechanisms and did not include many developing countries [May, 2010, p. 249]. Different countries have had many different rules and standards, and it is important to remember that each country defines specific forms of IP in different ways that reflect historical differences in their laws, legal traditions, and political evolution [Dixon and Greenhalgh, 2002, p. 44]. During the Uruguay round of trade negotiations from 1986 to 1994, the United States and other developed nations insisted on the establishment of a new treaty on the Trade-Related Aspects of Intellectual Property Rights, which World Trade Organization members would be obliged to accept. TRIPs requires countries to provide a minimum level of intellectual property protection and adhere to the Berne

and Paris Conventions. Special concessions were also negotiated for developing countries that need time to amend IPR laws in order to conform to the minimum standards [May, 2010].

As far as copyrights are concerned within the agreements mentioned above, it should be noted that they protect the expression of an idea. Copyright protection is provided to authors of original works, including literary, artistic, and scientific works. This includes books, movies, television programs, music, magazines, photographs and even software and databases in a growing number of countries. Copyrights generally allow the owner to prevent the unauthorized reproduction, distribution, and sale of original work. The TRIPs agreement of the WTO requires members to offer copyright protection that lasts at least the life of the author plus 50 years [Helfer, 2004]. In the United States and Europe, protection lasts for the life of the author plus 70 years. Lengths of copyright protection have grown longer in the last 100 years while the value of trade in copyrighted products has sprung. [Spinello & Bottis, 2009].

In Greece legal protection of the intellectual property was delayed. The penal law of 1835 determined the reproduction of books and any other printed documents and music compositions in case it took place without the creator's consensus as a particular criminal offence. At the same time, within this law, stealing was defined as the detraction of mobile objects including intellectual pieces of work. However, these provisions were far from providing complete and effective protection.

The first plenary law on the intellectual property, passed in 1920, asserted that intellectual work was protected during the author's lifetime and for 50 years after the author's death. Moreover, in the same year Greece joined the Berne Convention of 1886. The law 2387/1920 was modified several times in order to correspond in newer needs, and was replaced completely by the law 2121/1993, which brought plenty innovations in the system of protection. According to the latter law, intellectual property lasts as long as the life of the author plus 70 years [Koumados, 2002]. At the same time from the beginning of the nineties has begun the harmonization of intellectual property law, in the context of European Community, by the publication of repeated directives which regulate in an aggregate way several aspects of intellectual property for all member states [Khan, 2002]. Today the matter is regulated by the Greek Copyright Law 2121/1993 as last amended by the law 3057/2002, the implementation of the Directive 2001/29 EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society and other provisions [Maradola, 2002].

To date, the most common process for the author's assurance and the fatherhood's proof was the deposit of the intellectual work with a notary. In addition, it could be done by mailing a registered letter with sender and recipient the author himself (or even a third person as a recipient), who should keep the receipt and maintain the letter closed. The digital environment offers the possibility of great storage of information and the internet facilitates the dissemination of such information [May, 2010, p. 70]. This combination has led to the creation of work the use of which takes place in a great degree online. In this context online registration is called to cover the needs created in the new order of things.

## ***2.2 Economic aspects***

In a global economy IPRs have become a more critical issue both for those nations that own patents, copyrights and so on and for those nations that seek to use them to produce goods and services. Intellectual efforts create new technologies, describe new ways of doing things, develop new products and services, and expand the cultural richness of society. They result in intellectual assets, or pieces of information, that have economic value if put into use in the marketplace [Maskus, 2000, p. 27]. Such assets are called intellectual property to the extent they bear recognized ownership. Protection of intellectual property is vital to a healthy economy, to the preservation of artistic and creative works for all to enjoy and to the creation of new technologies. When artists are confident in their ownership of their creations, they feel able to make them available to a larger audience [Khan, 2002]. The wider the distribution the more reasonable the pricing, which in turn encourages people to go out and buy, read or watch the work.

When a government provides creators with a legal, but temporary, monopoly, they can exclude people from accessing their work without paying for it. Creators are remunerated for their effort by gaining adequate returns on their investment in generating intellectual property [May, 2010, p. 257]. Much of the revenue that comes from the appreciation and willingness to watch a creative work goes back to all who worked to make the original vision a reality. The economic returns to creating them depend on their costs of creation, their desirability to potential users, the structure of markets in which they are sold, and the legal rights established to permit property owners to control their use [Boldrin and Levine, 2002]. IPRs, therefore, provide incentives for creativity and innovation. As a result, consumers worldwide supposedly get a wider variety of new products at reasonable prices. IPR enforcement also helps provide consumers with higher quality and safer products than would otherwise be the case, and countries that protect intellectual property tend to benefit from more technology transfer [May, 2010, p. 257].

Creative works provide social, cultural, and economic benefits that society wishes to secure. These works involve investment costs, including training, time, materials and technology acquisition. Moreover, marketing copyrighted products requires costly investment that is more readily recouped under the greater certainty provided by protection. If other members of society were allowed to free ride on the works without compensating their creators, the incentives to create would be severely dampened [Lemley, 2004]. Static economic efficiency might be achieved at the cost of lower growth in cultural identity and reduced investment in “industrially useful” expression such as software. At the same time, providing exclusive rights limits the dissemination of literary works and raises static costs of education, research, and entertainment. The copyright system reflects a compromise between these difficulties, attempting to balance the needs of creators with society’s interests in wide access to the results of their efforts.

Thus, many of the economic benefits of an information society flow to those who own the information and knowledge resources which have been rendered as intellectual property rather than to those whose need for such information and knowledge might be greater and this leads officials to struggle over when and under what conditions these rights can be overridden to protect the general public and the poor [May, 2010]. In setting rules governing intellectual property rights, societies must strike a balance between the needs of inventors to control exploitation of their new information and the needs of users, including consumers and potential competitors working to develop follow-on inventions and innovations. “Stated another way, the system should find an appropriate balance between creating and disseminating intellectual property” [Maskus, 2000, p. 9].

Considering the copyright protection not really important or a simple linear function can begin to erode or even eliminate the intellectual property rights accorded to creators [Copyright Alliance, 2011]. Setting the proper level of intellectual property protection requires a proper balancing act [Boyle, 1996, p. 55] and it is crucial to be considered as the keystone in the whole process. The power that stems from the ownership and control of particular innovations and technologies may allow certain agents to maximize their influence through the control of specific knowledge-based resources, but also allows these preferred actors to enhance their advantages by the legitimization of their interest through law. At this point the conflict between arguments for the protection of private rights of owners and a notion of the general interest represented by a wider public domain should be highlighted [May, 2010, p. 87].

Knowledge and technology form a critical basis of wealth and power. In this era of global competition, individuals, firms, and nations understand that knowledge and technology confer competitive advantage. That the protection of IPRs has

risen to the status of a major foreign policy concern for the United States and many other countries is not surprising. The knowledge structure, like the production structure, the finance structure, and the security structure, clearly constrains the options and conditions the behavior of individuals, firms, and nations, and therefore affects the wealth and power they enjoy [Dixon and Greenhalgh, 2002]. The knowledge structure has high stakes as it sets parameters for which companies and economies will turn innovation into economic benefits, such as higher productivity, market share, and increased exports. It also helps determine the distribution of benefits from innovation, such as better goods and services, lower prices, competition, and productive capacity [May, 2010].

The preceding description captures the essence of the argument for intellectual property rights in a closed economy [Maskus, 2000, p. 10]. The situation is more complicated in a world of many countries that are linked by trade and investment. The lesson that one derives from this aspect of the economic history of Europe and America is that intellectual property rights best promoted the progress of science and arts when they evolved in tandem with other institutions and in accordance with the needs and interests of social and economic development in each nation [Khan, 2002, p. 10]. In short, the historical record suggests that appropriate policies towards intellectual property are not independent of the level of development or of the overall institutional environment.

### **3. The International Experience**

Before presenting the international projects that come from the US and the UK environment it is judged appropriate to give some more details on which was the threshold of copyright legislation.

#### **3.1 USA**

In the US the earliest federal statute to protect the product of authors was approved in 1790 [Hughes, 1988, p. 27 27; Spinello & Bottis, 2009, p. 32]. Policy makers felt that copyright protection would serve to increase the flow of learning and information and by encouraging publication would contribute to democratic principles of free speech. The protections provided to authors under copyrights were much more limited than those provided by the laws in many European countries based on moral rights. By 1910 the original copyright holder was granted derivative rights such as to translations of literary works into other languages, to performances and the rights to adapt musical works, among others. Congress also lengthened the term of copyright several times, although by 1890 the term of copyright protection in Greece and the United States were the most abbreviated in the world [Khan, 2002, p. 38].

From the USA's context two indicative examples are mentioned below. The first one is that of the Copyright Alliance and the Writers Guild of America, West (WGAW). It should be noted that except for the WGAW there is also the Writers Guild of America East (WGAE). The two guilds work collectively on national agreements and independently on work pertaining to their region.

The Copyright Alliance ([www.copyrightalliance.org](http://www.copyrightalliance.org)) is a non-profit, non-partisan educational organization dedicated to the value of copyright as an agent for creativity, jobs and growth. Its efforts are based on the belief that those who create, render and publish copyrighted works rely on the copyright law and its enforcement, for their creative and financial success. Copyright Alliance is composed from artists' unions to major publishers. All of its members are committed to promoting the cultural and economic benefits of copyright, as well as providing information and resources on the contributions of copyright. At the same time a great variety of creative works are represented, from songwriters to recording artists and software developers. Some of its main principles are to enrich their culture through incentives to create and disseminate new and innovative creative works, to advance educational programs in order to teach the value of strong copyright, and to promote the progress of creativity and free expression.

The Writers Guild of America, West ([www.wga.org](http://www.wga.org)), is a labor union composed of thousands of writers for television shows, movies, news programs, documentaries, animation, and new media. Their primary duty is to represent their members in negotiations with film and television producers to ensure the rights of screen, television, and new media writers. Because of the WGAW's long-term efforts, writers receive pension and health coverage, and their financial and creative rights are protected. The WGAW Registry is the world's leading screenplay registration service, registering more than 65,000 pieces of literary material every year. Since 1927, the Registry has aided in the creation of legal evidence and is a vital instrument of the Guild's service to writers. Material that is registered online is kept on file for five years. Registrations may be renewed within three months of the expiration date for additional five-year periods. Any material not renewed is being destroyed and purged from the Registry.

### 3.2 UK

In the UK between 1735 and 1875 fourteen Acts of Parliament amended copyright legislation and copyrights were extended to sheet music, maps, books, paintings, dramatic works, lectures outside of educational institutions and other forms of intellectual work [Khan, 2002]. Copyright owners had no remedies at law unless they complied with a number of stipulations which included registration, the payment of fees, the delivery of free copies of every edition to the British Museum, as well as complimentary copies for four libraries. The term of the

copyright in books was for the longer of 42 years from publication or the lifetime of the author plus seven years, and after the death of the author a compulsory license could be issued to ensure that works of sufficient public benefit would be published [Dixon and Greenhalgh, 2002].

The UK Copyright Service (UKCS) is the established copyright registration facility that will be presented below from the UK context. In early 1999 the UKCS ([www.copyrightservice.co.uk](http://www.copyrightservice.co.uk)) was conceived as a result of concerns about the quality of copyright evidence and officially opened its doors in April 2000. Since then it has taken up the role of providing a center for intellectual property registration in the UK. The UKCS grew rapidly between 2000 and 2004, and over that period also received growing interest from international copyright owners.

In June 2004, all company systems were migrated to dedicated self hosted servers, ensuring the very best quality and security for clients and site visitors. It also heralded the launch of a new web site, which allowed clients to access forms and documents previously only available by post.

In 2005, it launched a new, high security, online registration facility offering virtually unlimited upload sizes and in 2007 online registration renewals were launched.

Today, the UKCS is a well established service in the area of copyright protection which protects the work of thousands of copyright owners – from writers to web site developers – from all over the world, and operates fast, comprehensive and secure registration facilities that provide strong copyright evidence. Registered material can be kept on file for five or ten years and registrations may be renewed upon expiration.

## **4. The Website and the Application**

### ***4.1 The renewal***

SGG is the only professional guild for screenwriters in Greece. Members of the guild are the founding members as well as those who are able to acquire this attribute by submitting an application. Guild's members are distinguished in regular, apprentice and honorary. The professional condition in order to become a regular member of Guild is the proven exercise of the screenwriter's profession and particularly the subscription of at least one according to the conditions described in Guild's memorandum. Indicatively, a prospective member is expected to have already written screenplays for two fiction films appeared either on cinema or at an international festival, a script for twenty television episodes that has been transmitted in national level or screenplays for six cinematographic documentaries. As expected, the conditions for one to be an apprentice member are less.

The website [www.senariografoi.gr](http://www.senariografoi.gr) has been publicly available since June 2004. Today, almost seven years later, it has vindicated the expectations of founders having achieved into practice to create new possibilities of communication and at the same time to concern both the professionals of the audiovisual field and the visitors interested. One more objective that has been accomplished was to have a significant number of visitors which would increase year by year. Statistical data are adequate in order to substantiate that the progressive increase of visitors is already apparent from the first year on. Indicatively it is reported that in 2006 visits showed an incredible increase of 103.6% compared to that of 2005.

After a period of hard work, in 2011 the renewed website of the Scriptwriters' Guild of Greece was finally ready. The construction and development parts have been completed successfully and new content is being added every day. Special attention has been given to the informative and interactive aspects of the website. The Members' database and the scripts database are two of the most interesting parts of the website, along with the FSE's section, exclusively dedicated to the Federation of Scriptwriters in Europe. Moreover, apart from the pages dedicated to SGG, its organization chart, the members' database along with their biography, FSE's presentation and legal issues, the website has also hosted much information about seminars, workshops, announcements and resolutions, hundreds of images, many links to other websites – such as script libraries – and more than 1,500 references, either internal or external.

The most important service of the renewed website is the online script registration. After the first two month period in operation of the new service 63 users have been registered and 48 of them have chosen to proceed with full registration. However, the service has accepted criticism that concerns, in the first place, the duration of registration validity, as well as the registration fee since the process via a notary takes place once and is valid forever according to the relevant law (2121/1993). Taking this argument into consideration, on Monday, July 18, SGG announced the expansion of the registration's duration. From that moment on the registration will be valid for a lifetime and not just for ten years as it used to be. It would be useful to note that the registration fee provides a Registration Certificate, legal evidence and lifetime storage for the material. It also helps maintain the overhead for the department, including the maintenance of the confidential facility where the material is stored.

#### ***4.2 Core and critical features***

Since its inception in 1991, the Web has changed dramatically. What started as a hypertext system for distributing scientific documents has changed into a ubiquitous global network for exchanging all kinds of data. Along with the content, the presentation of information in the Web has changed. Originally, Web servers



acted like file servers that produced stored documents on demand. Nowadays, most Web pages are computed on the fly according to user profiles, language and image preferences, or the latest news. Not only are those pages generated dynamically, but they also support all sorts of interaction [Thiemann, 2005].

Clearly, the implementation of all those interactive services requires substantial effort for developing software that runs on the Web servers or associated application servers. Despite the fact that it seems easy to program dynamic Web pages, it turns out that programming reliable interactive Web services is very hard. The process for the development of an application like online script registration was proved technically difficult and quite lengthy. The developer had to take under consideration the right way for every step of the registration, so as to make the application easy and usable for all kinds of users willing to register their script in no more than 5 easy steps. In addition, there were considerations regarding security and synchronizing accesses to shared resources on the server (database transactions, in particular) among different session threads [Meijer, Leijen and Hook, 1998]. At the same time, the developer had to predict any possible mistakes the user might make and foresee both the steps and the user's reaction in order to surpass a certain mistake. All these steps were made with the indispensable assistance from members of the Scriptwriters Guild of Greece, so that any practical and legal detail could be taken into account.

Since the introduction of the Web there has been a constant migration of computational power from the server to the client [Thiemann, 2005]. Server side scripting provides critical interactive data entry capabilities and dynamically generated content. With server-side scripting, completing an activity involves sending information to another computer (server) across the internet [Yu et al., 2007]. The server then runs a program that processes the information and returns the results, typically a webpage. Server-side scripting languages include ASP and PHP. Search engines use server-side processing and when a keyword is sent, a program on a server matches the word or phrase entered against an index of website content. On the other hand, client side scripting extends the interaction paradigm by allowing content designers to specify reactive behaviors in their web pages in a much more modular and efficient fashion. Using client-side scripting it is possible to build interactive web pages that do not need round trips to the server for every user event. The web browser exposes itself to the script via an object model (DOM) which means that scripts can add and remove page content [Meijer, Leijen and Hook, 1998].

The SGG site operation is based on both client-side scripting and server-client scripting. Client-side scripting enables interaction within a webpage. The code required to process user-input is downloaded and compiled by the browser or

plug-in. An example of a client-side interaction is the possibility to locally rearrange the appearance of an HTML element when the mouse is positioned over the element without the need of generating a completely new page on the server. Client-side scripting languages include the widely used JavaScript (ECMAScript) which is also the dominant client-side language for this particular project, especially utilizing the jquery library. In addition to the scripting techniques mentioned above a relational database structure was built on a web-server for the sake of data storage using the mysql relational database management system. Finally, ajax technology is used to make direct requests to the web server and the database without reloading the page.

### ***4.3 The Registration process***

If someone wants to register as a user, he has two options. The first option is simple registration where one doesn't need to give any personal details. The second option is full registration where one is asked to give personal details, such as name, address, date of birth etc. This process is necessary as far as online script registration is concerned. At this point it should be noted that identification problems emerge. Identification is rendered essential as for the registration process. In the online environment users can declare any elements they wish. However, as far as the registration of intellectual property foes, one should be extremely careful and this is the reason why even the id number is required.

Any file may be registered to assist the user in documenting the creation of his work. Some examples of material accepted for registration include scripts, treatments, synopses, documentaries, animation, plays, novels, short stories, biographies, poems, lyrics, fairytales and so on. The registration process places preventative measures against plagiarism or unauthorized use of an author's material. While someone else may have the same storyline or idea in his or her material, the evidence lies in the presentation of one's work. Registering one's work does not disallow others from having a similar storyline or theme; rather, it potentially discourages others from using that work without permission. It should be mentioned that though the Registry cannot prevent plagiarism, it can produce the registered material, as well as confirm the date of registration. It creates legal evidence for the material that establishes a date for the material's existence.

Only the authorized beneficiary may request access to records or information pertaining to registered material. All requests must be in writing from authors regarding their own work and must be accompanied by ID evidence. Unless the user designates otherwise, personal information will be kept confidential by the Registry and will not be disclosed to outside organizations for any purpose. Requests may be submitted by mail, facsimile or delivered in person. Since the primary purpose of registration is to establish the completion date of the original

work once material is registered, the file cannot be changed in any way. New drafts should be registered when significant additions have been made.

As far as copies of registered material are concerned, copies of material may be purchased upon written request by one or more of the listed authors, identified by ID. In case an author is deceased, proof of death and consent of the representative of the heir must be presented in order to obtain a copy of the material. Duplications of material submitted in person or by mail are photocopied and available for pick-up or sent via certified mail approximately two weeks after the request is made. Duplications of material submitted online are burned onto CDs and available for pick-up or can be sent via certified mail approximately one week after the request is made. In no event, except under these provisions, shall any deposited material, copies of deposited material, or information regarding deposited material be provided unless an official guild action, court order, or other legal process has been served.

Files are transferred directly to SGG. The upload is originated at the user's PC and will arrive at the SGG Registry's server. In mere moments one's material is secure behind SGG's firewall. Uploaded data does not reside on an intermediate server so as to avoid the danger of interception. In the final stage material submitted online is stored in a non-rewritable digital format in a secure location. In the following lines the end user interface of the online registration procedure is described step by step:

### *1. Registration*

In step 1 writers are asked to verify or change, if needed, the contact details, read and agree to the terms of service.

### *2. Submit*

In this step the user will be asked to enter details about the work that will be registered. These details are the title of the work, its type and the release medium. In order to submit the archive the writer will be prompted to browse and select the specific file for registration. One should then press the "browse button", find the file in the computer, choose it and press "open". If the format is not PDF, MS Word or Open Office Writer the work will not be accepted. Pressing the "next" button takes the user to the next step.

### *3. Confirmation*

This screen is about checking that all the details are correct. If any kind of correction is needed, the "edit" button at the bottom of the screen serves this purpose. Furthermore "Temporary Script File" accommodates those who want to download a copy of their work. If everything looks OK, one should press "I confirm work's details" and then proceed to the next step by pressing the "Continue" button.

#### *4. Payment*

The fourth step is "Payment" which is completed online by credit card. The transactions are insured by Paypal or credit card. By choosing "Immediate Payment by Credit Card" users are directed to Paypal. Once the transaction is completed they can proceed by choosing "Payment Completion Control". The last step is not available until the payment is authorized.

#### *5. Registration completion*

At this point the submitted work has been successfully registered and already is in guild's files. Finally, the writer receives a "Registration Certificate" with all the relevant details.

### **5. Conclusions**

At the time when intellectual property legislation was making the first steps people were not fully aware of its great importance as far as healthy economic growth was concerned. Over the years the situation gradually changed. The legal protection of intellectual property and its dissemination evolved and people came to realize that apart from the satisfaction that occurs for both the creator and the consumer there is also a strong relation to economic transactions that are necessary in the whole process. Nevertheless, the balance seems to be at stake as many people follow practices which put both economy and intellectual property in danger. It is a matter of great importance to understand that law itself cannot draw the line between protection and the public domain.

The digital age brings a multitude of opportunities for the creators of copyrighted works, as well as their producers and distributors. New business models are being developed every day to create, distribute and market artistic works. At this point it is the way in which technology is used and not technology itself that harms the creators of copyrighted works. Strong copyright protections encourage individual creators to take advantage of advances in digital technologies in order to protect their creative works. Technology and copyright protection need not be at odds with each other. Instead they both need to work to the benefit of all. The Web can now be used for purposes beyond information and entertainment purposes and the most indicative example for that is this application which allows online script registration. Intellectual property, economy and technology intertwine and designate both the instrumental role of technology and the potentials offered by the Web as far as evolution of applications is concerned.

Under these circumstances, SGG is continually reviewing the existing services to seek improvement where it can. According to the results of its pilot period the next steps concern the improvement of the application in order to serve in the better possible way the user's needs. Throughout this and the next year the de-

velopment team will be developing the new software systems that will provide further web based facilities for users. Moreover, it is essential, in order to achieve widespread use of service, to find ways of further promotion and make it widely known. At last as far as the institution is concerned it is critical to come up with ways to reinforce its institutional role aiming at the more effective protection of writers' rights as creators and professionals in the audiovisual industry.

## References

- Boldrin, M. and Levine, D., 2002. The case against intellectual property. *American Economic Review (Papers and Proceedings)*, 92 (2), pp. 209–212.
- Boyle, J., 1996. Intellectual Property Policy Online: A young person's guide. *Harvard Journal of Law & Technology*, 10 (1), pp. 47–111.
- Copyright Alliance, 2011. [online] Available at: <http://www.copyrightalliance.org/> [Accessed 20 September 2011].
- Dixon, P. and Greenhalgh, C., 2002. The Economics of Intellectual Property: A Review to Identify Themes for Future Research, Oxford Intellectual Property Research Centre Working Paper Series No 5. Available at: <http://www.oiprc.ox.ac.uk/EJWP0502.pdf> [Accessed 30 May 2011].
- Helfer, L. R., 2004. Regime Shifting: The TRIPs Agreement and New Dynamics of International Intellectual Property Lawmaking. *Yale Journal of International Law*, 29, pp. 1–83.
- Hughes, J., 1988. The Philosophy of Intellectual Property. *Georgetown Law Journal*, 77, pp. 287–366.
- Kawohl, F., 2008. Commentary on German federal copyright directives (1837–1869). In Bently L. and Kretschmer M. (eds.). 2008. *Primary Sources on Copyright (1450–1900)*. Ch. 8.
- Khan, Z., 2002. Intellectual Property and Economic Development: Lessons from American and European History. *Commission on Intellectual Property Rights*, Study Paper. [online] Available at: [http://www.cipr.org.uk/papers/pdfs/study\\_papers/sp1a\\_khan\\_study.pdf](http://www.cipr.org.uk/papers/pdfs/study_papers/sp1a_khan_study.pdf) [Accessed 25 September 2011].
- Koumantos, G., 2002. *Intellectual Property*. 8th ed. Athens – Komotini, Sakkoulas (in Greek).
- Lee, E. A., 2005. What are the Key Challenges in Embedded Software? *Guest Editorial in System Design Frontier*, 2 (1).
- Lemley, M., 2005. Property, Intellectual Property, and Free Riding. *Texas Law Review*, 83.

Marandola, M., 2002. The Greek copyright law, actual problems for libraries and archives. Available at: <http://conference.teiser.gr> [Accessed 30 May 2011].

Maskus, K. E., 2000. *Intellectual Property Rights in the Global Economy*, Washington D.C., The Institute for International Economics.

May, C., 2010. *The global political economy of intellectual property rights: the new enclosures*. 2<sup>nd</sup> ed. London, Routledge.

Meijer, E., Leijen, D. and Hook, J., 2002. Client Side Web Scripting with HaskellScript. [online] Available at: <http://research.microsoft.com/en-us/um/people/emeijer/papers/client-side-web-scripting.pdf> [Accessed 30 May 2011].

Oman, R. and Flacks, L., 1993. Berne Revision: the continuing drama, *Fordham Intellectual Property, Media and Entertainment Law Journal*, 4 (1), pp. 139-156.

Scriptwriters Guild of Greece, 2011. Available at: <http://senariografoi.gr/> [Accessed 30 September 2011].

Spinello R. & Bottis M., *A defense of Intellectual Property Rights*, Edward Elgar Publishing, 2009.

Thiemann, P., 2005. An Embedded Domain-Specific Language for Type- Safe Server-Side Web-Scripting. *ACM Transactions on Internet Technology*, 5 (1), pp. 1-46.

UK Copyright Service, 2011. Available at: <http://www.copyrightservice.co.uk/> [Accessed 30 September 2011].

Writers Guild of America, East, 2011. [online] Available at: <http://www.wgaeast.org/> [Accessed 25 September 2011].

Writers Guild of America, West, 2011. Available at: <http://www.wga.org/> [Accessed 30 September 2011].

Yu, D. A. et al., 2008. Better abstractions for secure server-side scripting. In: *Proceeding of the International Conference on World Wide Web*, pages 507-516.

# Digital disposition of a work: from technical protection measures to creative commons

---

---

Alexandra Giannopoulou

---

---

## Introduction

A steady Feature of the law has always been the aim to remain neutral and above technological progress, in order to remain applicable to all issues stemming from technological progress and thus, immune to threats. In the case of laws defining and protecting intellectual property, a reaction was necessary against all threats coming from the continuous technological progress. Intellectual property has grown to include many different artistic creations, as well as to include new uses of these creations, such as a digital disposition of a work<sup>1</sup>.

The core of the function of the Internet lies on sharing. Intellectual property rules are more “flexible” in the eyes of the users and the risk of being caught seems minimal. Since the simple word of the law did not have an effect on peoples’ attitudes, the legislator decided to use technology in order to eliminate the problems originating from the evolution of technology. The publisher Charles Clark, in his most memorable phrase concluded that “the answer to the machine is the machine”<sup>2</sup>. In other words, he suggested that all intellectual property problems related to new technologies can only be solved by the use of technology.

This is how the well-known technological measures were established in all kinds of creations. Since the very birth of copyright, there have always been legally controlled forms of getting access to protected works and objects of related rights, such as buying copies of works and records, lending books from libraries, buying entrance fees for cinemas, theatre, concert halls and exhibition halls etc.<sup>3</sup>

- 
1. Vagena E., *Technological protection and digital administration of intellectual property* (in Greek), Nomiki Vivliothiki, 2010, p.1.
  2. Charles Clark, The answer to the machine, is the machine, in Hugenholtz B., *The future of copyright in a digital environment*, Kluwer law International, 1996, p.139-146.
  3. M. Fiscor, Protection of ‘DRM’ under the WIPO ‘Internet Treaties’: Interpretation, Implementation and Application in Irini A. Stamatoudi, *Copyright enforcement and the internet*, Kluwer 2010, p. 283.

Regarding the case of the internet, many mechanisms appeared in order to secure the digital disposition of creations or in order to prevent and control certain uses of creations. Severine Dusollier graphically describes this attempt as the “will of the author to reinforce their power over their intellectual possessions, to push away the intruders. It is an effort to reinstall their power over their creations which was lost by the digital mutation and other technological developments. In an era when copying is easy and the conscience of copying has died out, technical measures are nothing more than the “lost morality” of the user of digital creations”<sup>4</sup>.

But since the fate of technology is to be rapidly updated and, thus, outdated, the risks of circumventing the technical measures created to protect intellectual property rights of creations could not be ignored by the legislator. In order to put a legal fence of protection over the technical protection measures, international and national rules were created to penalize acts of circumvention.

## 1. Typology of technical protection measures

An official categorization of technical protection measures<sup>5</sup> does not exist. However, several opinions exist by various scholars in an attempt to provide the most accurate description possible. The fear of oversimplifying these measures as well as the constant evolution of technology constitutes this task even more difficult. The most widely accepted system of classification is that which takes as a distinctive criterion the function of each technological measure<sup>6</sup>.

According to the aforementioned classification theory, there are three major categories of technical protection measures:

### *a) Technical measures that control the access to works*

It consists of systems integrated in a creation so as to control the access to the original creation or even the making of copies of the original creation. These systems lock the creation and only the user with the proper password can get access. The anti-copying systems work in a way so as to make the illicit copying of a creation almost impossible. One of the most known examples of the anti-copying devices is the region code restrictions of DVDs. In other words, the globe is divided in 6 regions which do not interact when it comes to playing DVDs acquired from a specific region code to another. As most of the technological measures, this function can be circumvented. In addition, another use is to not obstruct the

---

4. Dusollier S. (2007), *Droit d'auteur et protection des œuvres dans l'univers numérique*, Larcier, p. 37.

5. Hereinafter TPMs.

6. Dusollier S., *Droit d'auteur et protection des œuvres dans l'univers numérique*, op.cit., p. 40.



original access to a creation but the graduated completion of this access. The use of *beta versions* of various programs online is the most common example. The user can store a particular program for use to his computer for a specific amount of time. Afterwards, and according to the amount of satisfaction, the user can decide to acquire a copy of the program in question or not<sup>7</sup>.

### ***b) Technical measures that control the uses of works***

This type of technical measures consist of restrictions and controls over the potential uses of a creation. There are certain technical measures that authorize copying, for example, but in a restricted environment only. Others allow a specific number of copies or control the quality of the copied creation so as it can no longer be useful for further exploitation. The most common example of such measures can be found in the iTunes technology, whose particularity will be discussed further below.

### ***c) Technical identification measures***

The identification measures assemble all the information that constitutes the identity of each creation. Hence, they can provide information not only about the name of the creation and its author, but also information about the legal status of the creation. This information plays the role of the matriculation plaques of digital objects in the “avenues of information”<sup>8</sup>. The use of these measures is manifold. The identification informs each potential user for the nature of the creation as well as for the uses that are legally permitted by the author. It also works as a guide to the computer that analyzes the data and accordingly grants or denies specific uses to third parties.

These technical measures apply to digitalized creations as a second layer of protection against intellectual property threats. Soon enough, they were recognized as legitimate measures from the international legal community and their protection was considered necessary.

7. Vagena, E., *Technological protection and digital administration of intellectual property*, op.cit., p. 19.

8. See Vagena, E., *Technological protection and digital administration of intellectual property*, op.cit., p. 20 as well as Dusollier, S., *Droit d'auteur et protection des œuvres dans l'univers numérique*, op.cit., p. 40. This metaphor was originally used by Ginsburg J., “Putting cars on the “Information Highway”: authors, exploiters and copyright in cyberspace”, in Hugenholtz, B., (ed.), *The future of copyright in a digital environment*, Kluwer, 1996, p. 189-219.

## 2. The legality of technical protection measures

Unfortunately, for the media industry technical protection measures are inherently fallible as ingenious hackers always find ways to circumvent them<sup>9</sup>. In an effort to offset this vulnerability, these measures attained legal protection and such tampering with them induced legal sanctions.

### *a) Legal protection for technical protection measures*

The legislative foundation for TPMs was created through the two WIPO Internet Treaties on 1996. The expression Internet Treaties refers to the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, adopted on 20 December 1996 by the WIPO Diplomatic Conference “on certain Copyright and Neighboring Rights Questions”<sup>10</sup>.

According to article 11 of the WIPO Copyright Treaty, “*contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law*”<sup>11</sup>. Article 18 of the WIPO Diplomatic Conference deals with the same issues using an almost identical language.

The European Union, in conjunction with the aforementioned Treaties, protects in its turn the technical protection measures. The Directive 2001/29/EC of 22 May 2001 “on the harmonization of certain aspects of copyright and related rights in the information society” installs a similar protection system.

In the case of the United States, a law protecting technical protection systems was incorporated in the Digital Millennium Copyright Act on 1998. These provisions also integrate the conditions set by the WIPO Internet Treaties.

The international community demanded from all contracting parties an “adequate” and “effective” protection regarding technical protection measures. This protection covers all acts of circumvention as well as preparatory acts of such cir-

---

9. Bechtold S. (2004), *Digital rights management in the United States and Europe*, Am. J.Comp. L., 52, 323,331 cited in Winn J. & Jondet N. (2009), *A new deal for end users? Lessons from a French innovation in the regulation of interoperability*, 51 William & Mary Law Review 547, 2009.

10. Fiscor M., *Protection of ‘DRM’ under the WIPO ‘Internet Treaties’: interpretation, implementation and application*, op. cit., p. 257.

11. The text of the treaty is available online in the WIPO site: <[http://www.wipo.int/treaties/ip/ip/wct/trtdocs\\_wo033.html#P87\\_12240](http://www.wipo.int/treaties/ip/ip/wct/trtdocs_wo033.html#P87_12240)>.

cumvention. The difficulty in clearly defining the terms used in laws protecting technical protection measures led many cases to be clarified by courts.

The term “effective” when referring to technical protection measures needs further explanation in order to determine the criteria that define the nature of its effectiveness. It has to be noted though, as it has been pointed out by the WIPO Guide to the WCT that infallibility is not a criterion of effectiveness. According to the Guide, such interpretation would be absurd since the objective of the provision is precisely guaranteeing protection against acts of circumvention, which “by definition” must be regarded to be possible also in case of effective technological measure (since if it were possible, no protection would be needed)<sup>12</sup>.

The Helsinki District Court, based on a theory applied in American courts, created a test of effectiveness of its own. According to the Court, if the software used to circumvent protected material is made available only to a limited amount of online sources, only then the technical protection measure can be characterized as effective. This case caused a lot of excitement in the copyleft<sup>13</sup> movement but it was quickly overturned by the Helsinki Court of Appeal with the justification that the technical protection measure is suitable to achieve its objective *in the normal course of operation*.

### ***b) Controversial application of technical protection measures***

The Mulholland Drive case illustrated the meaning of the obligation of respect of limitations and exceptions introduced by copyright law when applying technical protection measures. The infamous case was followed with great interest from scholars. The decision concluded that the right to private copying does not apply in the case of DVD films protected with TPMs. In other words, the owners of rights are not obligated to remove any TPM systems applied to the DVDs because such “an action would be in conflict with a normal exploitation of the work in question”. The Court of Cassation justified its decision<sup>14</sup> by claiming that a possible permission to make free copies of TPM-protected works could result in an illegal online distribution for other users. Various countries in Europe have dis-

12. Fiscor M., *Guide to the copyright and related rights treaties administered by WIPO* (Geneva, WIPO publication No 891 (E), 2003), 216 cited in Fiscor M., *Protection of ‘DRM’ under the WIPO ‘Internet Treaties’: interpretation, implementation and application*, op. cit., p. 270.

13. Copyleft is a play on the word copyright in order to describe the act of certain authors to offer *freely* to users the right to distribute copies and modify a work with the only condition that all later modified versions of the work will be distributed under the same rights.

14. Cour de cassation, 1<sup>ère</sup> chambre civile, 19 juin 2008 (pourvoi n° 07-14.277 F-P+B), rejet du pourvoi de cour d’appel de Paris, 4 avril 2007. Available on line (in French) <[http://www.legalis.net/spip.php?page=breves-article&id\\_article=1909](http://www.legalis.net/spip.php?page=breves-article&id_article=1909)>.

missed the claim of multiple copyleft advocates that the right to private copying is being obstructed by TPMs.

It would be convenient to defend the priority of TPMs over the legal exceptions introduced by international treaties and transposed in national laws. However, the importance of such exceptions should not be dismissed or ignored by technology. They do not constitute a “marketing option for the rights holders”<sup>15</sup>. In other words, it is not up to them to decide their applicability but only the legislator can decide the legality or not of a suppression of an exception.

The biggest enemy of TPMs is circumvention. However, the discussion has shifted lately to the legality of the so-called “jailbreaking”. This term concerns all acts resulting in allowing the user to upload unapproved or unofficial software to a hardware device. This act does not fall in the notion of circumvention whose illegality lies in the fact that authors want to keep control over the uses of their works. The particular case of jailbreaking raises the question of whether users have the right to remove restrictions over what type of software can be installed in a particular device.

Since July 2010, United States have given a solution to this problem in their national legislation. Namely, the Library of Congress included “jailbreaking” in the list of actions that constitute fair use and, thus, do not violate the Digital Millennium Copyright Act (DMCA). Although this decision --also called the iPhone case-- has given an answer to the problem of the legality of jailbreaking, in other countries this subject has yet to find an official resolute answer.

No matter how beneficial the use of TPMs is for the protection of the authors' rights, they sometimes constitute an obstacle to the spread of a work even for users who choose the legal road to purchase a work and do not recourse to illegal file sharing programs. Taking the example of the aforementioned region coding, it serves to control the release of films as well as their price but it is a barrier to individuals who purchase DVDs from different region codes expecting that they will work. Moreover, another example of how copyright industries do things in their own way concerns the accessibility of the legitimate digital downloading market. In fact, a large number of developing countries do not have access at all or even when they do, it is largely depleted.

---

15. Ginsburg J. and Gaubiac Y. (1998), “*Private copying in the digital environment*”, in Kabel, J. J.C. and Mom, G. (eds.), *Intellectual property and information law: essays in honor of Herman Cohen Jehoram*, Kluwer, Information Law series, No 6, p. 152. For a comment on the connection between fair use/private use (exceptions) and DRM, see Grodzinsky F. and Bottis M. (2007), *Fair Use/Private Use: Is it Fair?* ACM SIGCAS Computers and Society, vol. 37, issue 2, pp. 11-24.

It has been established that sometimes the purpose of some TPMs is not completely fulfilled, and that it can result to illegal behaviors such as illegal downloading. In these cases the question has to go even deeper in order to explore the possibility of different possible ways to keep control over works, without extremely restricting it to the point of excessive copyright control.

### 3. The existence of TPMs in the Creative Commons licenses

The goal of traditional legislation methods is to establish a sense of security regarding the digital fate of works by augmenting the control exercised by the author to their works using multiple technical or legal “tools”. The free movement constitutes the antipode of this system. It provides authors with the possibility of digital disposition of their work using the same legal means with the difference of conceding more power to the users accessing a particular work. This movement has a unique effect globally because the right to access to information has become one of the dominant rights in matters of intellectual property and the restrictions imposed by the current legislations repel many users<sup>16</sup>.

#### a) *The function of the Creative Commons licenses*

The regime of the Creative Commons licenses<sup>17</sup> lies on the proprietary system that characterizes the current legislation. However, the licenses try in the same time to “stimulate another practice of copyright in order to provide a different image than that of a system which restrains creation and access to works”<sup>18</sup>. It essentially consists of private agreements which apply on the top of the law as a form of exploitation of rights emerging from copyright. The CC licenses have become a de facto standard for open content licensing.

According to the CC website<sup>19</sup> “Creative Commons licenses are expressed in three different layers or formats: the Commons deed (human-readable code), the Legal Code (lawyer-readable code) and the metadata (machine readable code)”<sup>20</sup>. Each li-

16. As Barlow and Brand have stated in the first Hackers Conference in 1984: “Information wants to be free”.

17. See Dulong, de Rosnay M., “Creative Commons licenses legal pitfalls: incompatibilities and solutions”, Institute of Information Law University of Amsterdam, available online <[http://www.ivir.nl/creativecommons/CC\\_Licenses\\_Legal\\_Pitfalls\\_2010.pdf](http://www.ivir.nl/creativecommons/CC_Licenses_Legal_Pitfalls_2010.pdf)>.

18. Dussolier S., “Les licences Creative Commons: Les outils du maître à l’assaut de la maison du maître”, Propriétés Intellectuelles, 2006, n°18, p.10.

19. <<http://wiki.creativecommons.org/FAQ>>.

20. i) a human readable summary of the license’s core freedoms and optional restrictions, ii) the legal code, which constitutes the full text of the license and iii) a machine readable code em-

cense is constituted by the “core clauses”, which are similar to all licenses, and by the optional elements that are chosen by the license chooser interface and lead to a puzzle of elements. The assemblage of all elements (optional and non optional) leads to one of the six licenses currently available online. According to the licensor’s wishes, the license can include some, all or none of the optional elements. The six licenses available are: attribution (BY), attribution-share alike (BY-SA), attribution-non derivative works (BY-SA-ND), attribution- non derivatives-non commercial (BY-ND-NC), attribution-non commercial (BY-NC) and attribution-non commercial- share alike (BY-NC-SA). During the creation of the license, the licensor can add additional information in the form of metadata such as the name and contact information for the author. The six combinations forming a CC license, available in all three formats, constitute the heart of the licenses.

### ***b) The anti-TPM provision and a new era for metadata***

In its effort to keep intact the freedom of the licensed works, the Creative Commons organization inserted a particular restriction to the limitations clause. According to it, the acceptant of the license “may not impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You [the acceptant of the license] to exercise the rights granted to that recipient under the terms of the License”<sup>21</sup>. This is a direct expression of the anti-TPM position of the organization, by supporting that a controlled access or use of a work goes against the basic ideology of the organization and the freedom granted by all creative commons licenses.

However, there have been some doubts expressed by an organization in the free software community, called Debian. According to their opinion, that kind of prohibition prevents licensees from distributing works in formats of their choice, even if this applies to TPM-protected formats. The example used was the possible distribution of CC content on Sony Playstation platforms. Debian proposal to resolve this problematic aspect of the CC licenses is called the “parallel distribution” proposal. It essentially consists of a provision that gives the right to licensees to distribute CC-licensed works into any kind of formats, protected or not, provided that at least one format of the work would not restrict another person’s exercise of rights under the license. This possible TPM policy change has been discussed during the versioning process, but has reverse been included in newest versions of the licenses because of the opposition of the creative commons community to the possibility of restricting freedom.

---

bedded in the HTML containing metadata to be processed by search engines to locate works according to their licensing conditions.

21. Such clauses are present in all Creative Commons licenses, art. 4a Restrictions.

The CC licenses' system "circumvents" the restricting applications of digital rights management in order to promote only their positive uses. The use of metadata is an easy way to attach a license to work in the digital environment. In addition, metadata can hold information about the author, pricing information, contact information or even the status of liberty granted by the author to the users.

The potential of metadata as a means of expressing rights related to content is huge and not yet exploited to its full extent. The priority place that legal metadata should have in the copyright management is underlined even by the European Copyright Directive: "Technological development will facilitate the distribution of works, notably on networks, and this will entail the need for right-holders to identify better the work or other subject-matter, the author or any other right-holder, and to provide information about the terms and conditions of use of the work or other subject-matter in order to render easier the management of rights attached to them. Right-holders should be encouraged to use markings..."<sup>22</sup>

The positive uses of legal metadata have been widely discussed in the case of the particular licenses. The most well known user- friendly application is the implementation of a special search engine that enables users to limit their searches down to only works whose authors have conceded certain rights (such as the right to make derivative works for example). In fact, Yahoo and Google have already incorporated a creative commons search engine option. Given the amount of information available online as well as the proliferation of liberty levels to different works, the possibility to use the legal status of a work as a search criterion is an indispensable tool for users. With the information provided by the metadata, users can easier contact the copyright owner for authorization, if the planned use of the work is not in the scope of rights described by the license embedded on the work.

Evidently, metadata cannot solve any liability issues stemming from the quality of information available online. The user does not, for example, have a way of verifying that the information is up-to-date and correct<sup>23</sup>.

One of the biggest challenges present regarding creative commons metadata is their relation to the function of collecting societies. The structures of the CC licenses as well as the language used in the contracts promote such collaboration.

---

22. Council Directive 2001/29, art. 55, 2001 O.J. (L 167) 10 (EC).

23. See Hietanen, H. and Dulong, de Rosnay M., "Legal metadata web applications: case Creative Commons", Author manuscript, published in "Symposium on Digital Semantic Content across Cultures, Paris, le Louvre: France". Available online <<http://halshs.archives-ouvertes.fr/docs/00/12/01/82/PDF/hietanen-DulongdeRosnay-Legal-Metadata-for-Semantic-Web-Applications.pdf>>.

Up until now collecting societies monopolized the royalties' management. The rise of Internet and of digital dispositions has shown the birth of competition.

The use of legal metadata could be the key to reform the management of authors' royalties. Collecting societies' uses could include cc works as well in order to manage their commercial uses and educate the users regarding the "level of openness" of a work. This way the notion of collective management takes a different form in order to include all works to the benefit of users.

From an economic point of view, creative commons metadata reduce transaction costs since they are self-explanatory. In other words, the user can proceed to the use (or re-use) of a work without requiring the assistance of third parties as specialists (such as lawyers or IT specialists). Even a possible collaboration with collecting societies will not augment the distribution costs of a work since there are no technical obstacles for rights' holders to exercise some of the individual rights, while being a member of a collecting society.

#### 4. Conclusion

According to the Creative Commons organization, their goal is "*to build a layer of reasonable, flexible copyright in the face of increasingly restrictive default rules*"<sup>24</sup>.

We have established that TPMs exist to reinforce the control over copyrighted material. There is no harm in trying to protect a work any way possible, but the fact is that this sometimes excessive protection reaches a point of obstructing regular uses of works.

The society should not reach to the point of constructing such barriers using the pretext of a sustainable economy serving the fight against piracy. The proliferation of "tolls" <sup>25</sup> as a means of controlling a work distributed through various ways (radio access, internet access, console access etc) will only lead to a further repulsion of the public towards the artists, while in the same time the distributors gain most of the profit.

The positive potential of metadata has shown that there can be alternative licensing schemes that will actually function in an open content environment. The collaboration of the existing traditional copyright industry with the open movement

---

24. History of Creative Commons, <<http://wiki.creativecommons.org/History>>.

25. Bruguère J.M. et Vivant, M., obs. sous TGI Nanterre 2 septembre 2003, Propr. Intell. 2003, No. 9 p. 464, cited in Vercken, G. et Vivant, M. «*Mesures techniques de protection sur le DVD, le test des trois étapes met en échec l'exception de copie privée*», Legipresse No. 214, rubrique Cours et Tribunaux, pp. 148-155.



can lead to the resolution of the copyright insecurity that governs the Internet distribution.

Any aggressive attempt to “govern” all possible distributions of works is eventually going to fail. Current copyright enforcement policies do not seem to grasp the meaning of Foucault’s saying that coercion cannot ensure compliance<sup>26</sup>. Since the goal of all technical measures is to achieve the optimum distribution of a work by minimizing the transaction costs and the potential copyright threats, it is imperative that decision makers start thinking outside the box.

---

26. “Governing people in the broad meaning of the word, governing people is not a way to force people to do what the governor wants; it is always a versatile equilibrium, with complementarity and conflicts between techniques which assure coercion and processes through which the self is constructed or modified by himself” Foucault, M., *About the beginning of the hermeneutics of the self: two lectures at Dartmouth*, 21 *Pol. Theory* 198, 203-204.

# **The old ethical problems in the new information society in Russia**

---

---

**Vitaly Gorokhov**

---

---

## **Free access to information as a precondition for development of democracy and social market economy**

In the second half of the 20<sup>th</sup> century it became particularly obvious that possession of information gives people great strength. In the totalitarian societies it also gives them power or a justification of power. If an individual comes out with criticism of the system, he can always be silenced on the grounds that he does not possess complete information. The strength of bureaucrat lies in that the higher he is on the bureaucratic ladder, the more information he has at his disposal.

In a totalitarian society, instead of free circulation and dissemination of dates, information moves through “closed channels”. It was false information that moves through “open” channels. At first, false information from the top echelons is intended for the peoples of other countries and for their own citizens, but later on this phenomenon penetrates all levels of the bureaucratic ladder, the top ones in particular.

In such a situation, where crucial correct information is lacking, it becomes impossible to influence and control the society, with or without computers. This was vividly demonstrated by a campaign for the automation of management of industries and individual enterprises, which used to be particularly vigorous in our country in the 70s – 80s years. All enterprises, institutes and ministries sought to by computers, but then did not know what to do with them. What is needed here is not just the design of separate hardware components and their adaptation for the convenience of handling, but planning (or rather reorganization) the human activity with integration of machine components into it. Only by the transition to the era of glasnost did the free movement of information in society create the necessary social prerequisites for the development in Russia of new information technologies and for passing on to a so-called new information society. These, however, were only *prerequisites*.

Attainment of this goal under conditions of total “information” devastation, long lasting disruption of normal communications and a lack of realistic (not false) statistics requires great material expenditures, as these disadvantages must be overcome. Our history shows that the priority of ideology over economy, and

often over mere common sense as well, is extremely costly. In the information sphere, this resulted in the lack of normal communication with the West. It also affected information exchange within the country.

Free access to information, including environmental one, is a necessary condition for development of democracy and social market economy. To take part in the process of making environmental decisions, the general public should have access to information. The old technocratic wave in post-Soviet society has choked itself under the conditions of emerging market economy and the reign of democracy. Russian citizens who had been silent till then began to voice violent protests against, for instance, the turning-over of the Siberian rivers, contamination of water reservoirs, illegal and insecure disposal of health-hazardous industrial waste.

Free information access and public discussion of controversial technological decisions put an end to hegemony of technocracy and expertocracy which had been fully backed by totalitarian society and, in their turn, had given a scientific substantiation of the communist leaders' plans and deeds. We leave in a new situation in this time. The rates of scientific and technological progress are so accelerated that environment fails to cushion man's impact on itself and «digest» man's industrial and domestic waste without the help from outside. The understanding of environment as a receptacle given by God at the Man's disposal transforms gradually into people's awareness of their oneness with Nature, impossibility for them to exist without environment, of its vulnerability and limitedness, dependence of its (as well as the people's) survival on the people's cautious attitude to environment. As we can see, the main contradiction of modern technological civilisation, noticed by cultural criticism of technology, is that modern technology, on the one hand, opens some unprecedented opportunities for the humanity to satisfy and even make up their own requirements, and, on the other hand, makes it possible to destruct the very basis of human existence that has seemed until recently a dreadful nightmare of sci-fi authors. The problems of humanisation of technology touch directly the very popular in the West philosophy of technology and ethical problems that are not enough being discussed in the Russian society. Therefore there is a possibility of a reappearance of technocratic thinking in Russia also in the new situation, which creates for us information society.

At this moment, Russia witnesses the revival of technocratic thinking in a new situation. The market economy, if not controlled by society and the government, is known to lead to a more harmful effect on environment and more impoverishment of the biggest part of the population. Under such economic conditions democracy inevitably transforms into arbitrary rule and anarchy. This is followed by natural resources robbery, if there are natural resources, and methodical de-

struction of environmental conditions of society. Ecological and environmental protection organisations stand in the way of profitable economic and technological projects, while the exhausted and many times robbed people are eager to raise the level of their own well-being up to at least bearable standard and are anxious about the fact that they are not allowed to the public revenues distribution rather than about environmental protection. Such conditions fertilise the technocratic tendencies to revive in society, especially if these technocratic illusions promise prompt enrichment to society and are backed by the technocratic lobby's propaganda. Today we can hear some notes of nostalgia of the time when one could practically without control and care for environmental effects utilise great resources to develop this or that strategic or politically important from the leaders' point of view directions of technology, the point of view that was reinforced, substantiated and often imposed by lobby-groups of experts. This is the domination of expertocracy or «system technocracy» [Lenk 1994].

Under conditions of the dominating totalitarian regime and commanding-administrative economic system of that time, the very idea of any legal or moral responsibility could never arise. Any information of pollution, not-sanctioned discharge and even local catastrophes that were inevitably connected with that kind of new machinery development without taking care of effects on health of the people on the planet and the biosphere of the Earth, was considered secret and never leaked to mass media. In all the countries over the world information on nuclear power system has been kept in completely intransparent technocratic structures. If such information became available for journalists, it was removed by strict censorship before it was published. Today is it possible to publish this information, but the technocratic lobby's propaganda receives many new informational possibilities in the information society to declare through the mass media this information as scientific or political irrelevant. It is very difficult for citizens to understand some scientific and technological details and to differentiate of the partially false and right information about for example the utilization of the radioactive waste from the nuclear power stations. The information society create not only a new possibilities for a free access and distribution of the important information but also to fabricate false or particularly misspelled data.

German philosopher of technology Hans Lenk said: "Although the human being is not the creator of nature but the latter's creature (s)he seems to be able to imitate and continue processes of creating: in a sense, humans create new materials, even new elements, artificial environments and imposing and very potent technical appliances, procedures and operations as well as systems. Is man nevertheless "the dominator and processor of nature" as the mathematician and philosopher Descartes had noted at the beginning of the era of enlightenment? On the other hand, man being a very tiny grain of dust in the cosmos extending billions of light

years cannot really feel elated as “the crown of creation” any longer: He had to experience in the history of Western science “several sorts of basic weaknesses and traumata” restricting the position of centrality and the respective conviction and complacency: loss of the astronomical centrality within the world (whether in our own planet system or galaxy or the cosmos at large), loss of the property of being “the objective and aim of creation” and the special position compared to other animals. Even the traditional opinion that he would be the being exclusively determined by reason had to be given up in the last century.

Nevertheless, the human being enjoys even today still a special position in the order of nature – in so predictions and powerful explanations by using its theories, by manipulating according to their knowledge great parts and objects of nature and materials rather successfully. Humans would use all this for the aims to “exploit” nature for reaching man-made goals etc. This “power” – which might lastly even figure as a negative destructive technological encroachment on parts of natural systems – would be an expression of her or his special position. *Power and knowledge engender responsibility* – a special responsibility of the knowing and powerful being.

This responsibility of the human being does not only pertain to human fellows as well as to the future but also to whole life-worlds including natural systems (ecosystems) of the so-called “spaceship earth”. This will also show up in the newly discovered and developed capability of being able to systematically and genetically change hereditary dispositions, or genetically to engender new biological kinds or even, e.g. so called chimaeras, mixtures out of different biological kinds.

Biotechnical engendering of clones is nowadays already possible, however not yet without mistakes and risks. Will humans now indeed become the technical “masters and dominators” over life and kinds amounting to being a sort of dominator of living nature? Will they play up as some sort of almighty beings in small proportions including potential fantasies of almightiness towards greater scales? Are humans allowed to change their hereditary stock or even “clone” human beings? Technical and gentechnological successes should not induce a new complacency or self-overestimation, a new technological hubris in a world and period evidencing evermore delimitations, side effects and impairments of natural systems connections, in particular those ones induced by human encroachments on nature. To be sure, only humans can know and explain “nature” and realize the Bible’s order, “Subdue earth!”. It is true that there was also the biblical imperative to cultivate, heed and preserve the Garden of Eden; yet the idea and imperative of *dominium terrae* is still very powerful, even practically almost dominating our relationship with nature. Instead of stewardship for nature we have domination and manipulation as a strategy. Did we take too literally this imperative of domination over

the earth, did we exaggerate it until the limits of the possible or even bearable or even go beyond these limits? In fact it is true, even today humans are subdued by natural laws, they remain – in spite of all their technological power – a tiny part or a powerless particle within the cosmos at large. Elated and especially required is this being at most by its knowledge and indeed also in the moral sense: regarding its responsibility for the future of humankind and lately even of the biosphere and the ecosystems of the planet. Relative power – and indeed destructive power in the first place – would engender a special responsibility for those beings and systems which are dependent on the technological encroachments, or notably on non-interfering. Nature itself will thus become an objective of human responsibility. Edward Teller, the so-called father of the hydrogen bomb, stated in an interview that “the scientist or technologist ought to apply everything he has understood and should not put limits on that: whatever you understand, you should also apply. Whether or not man is allowed to, or ought to make, apply, produce, initiate, carry though everything he has able to make, or he can make and do certainly comprises a specific and precarious ethical problem, indeed” [Lenk 2003, 26-28].

This is also acceptable for nanoethics and nanotechnology. Scientists believe that if nanotechnology makes it possible to model some process, the technologist ought to apply “everything he has understood”, ought to implement this process in reality. Our civilization would be inconceivable without the many things brought about by engineering. Engineers and designers have brought to life what once seemed incredible and fantastic (manned space flight, television, and so on), but they have also developed sophisticated means of mass destruction.

Although technology is *per se* ethically neutral, the engineer cannot be indifferent regarding its application. However, a humanistic or anti-humanistic orientation of an engineer does not only find expression under extreme circumstances, it also has its implications in the engineer’s attitude towards the users of the products or with respect to the environment. The primary aim of technology and technical activity is to be useful to man, and this principle must be followed both in general and in detail. You can hardly consider it good if an engineer has not done his best to ensure ease of use, safety, absence of noise and pollution, and other requirements placed on the installation, building, or machine that he had designed. Even if those have been engineered through the effort of a large team of professionals, the moral responsibility of each member of the team for the product as a whole should not be diluted. There is another important facet of the problem. Many current manufacturing processes in the mass production of food, drugs, agricultural products and the like are known to be harmful to man and to nature.

Today, the social responsibility of engineers and designers to society as a whole and to their clients is particularly local. While philosophers and scientists argue about the best way to transform the world, engineers and designers are actually transforming it, not always to the best advantage, and often to the detriment, of people, society, and even mankind as a whole. That is why the problems of scientific, technological and business ethics, social responsibility scientists and engineers play a more and more important role in modern technoscience and society [Mitcham, and Duval 2000].

This is first of all the existence of the developed scientific and engineering community and then the development of the self-consciousness of scientists and engineers through scientific and engineering education systems. It is also important to have in society the social structures and social institutions that support of the relevant and moral orientation of scientists and engineers. But these conditions do not else exist for the time being in nanoscience and nanotechnology. There is as yet no sustainable scientific and engineering are no special nanoethics courses in the system of nanoeducation and there is a lack of the necessary institutional support in the Russia. In Germany different aspects of scientific and engineering ethics are discussed and investigated already many years ago [Schwanke 1994].

This is the reason why nano-scale implantants are already implemented in the human organism and even in the human brain without satisfactory scientific explanation and technological manufacture and sale different nanoproducts [Müller 2006, Baumgartner 2006]. "Currently, special attention in the public risk debate is being paid to synthetic nanoparticles. A vast potential market for nano-based products is seen in this field. New products, based on new properties of nano-materials can be brought about in admixtures or specific applications of nanoparticles, for instance, e.g. in surface treatment, in cosmetics, or in sunscreens" [Grunwald 2008]. "The Food and Drug Administration (FDA) says the rising number of cosmetics, drugs and other products made using nanotechnology do not require special regulations or labelling. In the US, at least 300 consumer products, including sunscreen, toothpaste and shampoo are now made using nanotechnology, according to a Woodrow Wilson International Center for Scholars report. The FDA treats products made with nanotechnology in the same way as other products – requiring companies to prove their safety and efficacy before allowing them to come to market. However, some product categories, including cosmetics, foods and dietary supplements are not subject to FDA oversight before they are sold, which already worries some advocates. Producing them with nanotechnology adds another layer of concern. ... The group cites studies showing that certain nanoscale particles can cause inflammatory and immune system responses in animals" [NewScientistTech 2007] (see also [Nanotechnologie erober Markt 2004, Scientific Committee 2007]).

In the 17<sup>th</sup>-19<sup>th</sup> centuries human society outlined the understanding of scientific and technological progress as continuous improvement of society and nature on the basis of the growing capacity of scientific knowledge of the world. Up to the middle of the 20<sup>th</sup> century this illusion and relating to it cosmic, natural scientific and technological Utopias led to blurring up limits of human cognition and technological activity, to development of scientific and technological optimism concerning the chance to make human society happy with the help of more and more advanced achievements of science and technology. This belief in continuous scientific and technological progress, absolutisation of a value-free scientific research, illusion of actual «creatability» of the world on the basis of the obtained knowledge resulted in the emergence of a scientific religion, based mostly on the belief in the power of scientific knowledge and the progressive character of technological activity, grounded on this knowledge. There appeared an illusion that if technology has made the Man of an animal, then, combined with science, it could make a God out of Man, the Creator of not only artefacts but of matter, nature and life as well. Scientific and technological progress is subconsciously taken as a way beyond the limits of the possible. Such notions come back to philosophy of science and philosophy of technology of the late 19<sup>th</sup> – early 20<sup>th</sup> centuries, but it was Francis Bacon who had already first mentioned this in his works in the 17<sup>th</sup> century.

Since that time science was regarded as a means to multiply human knowledge aimed at creating man-made conditions and equipment to facilitate human life. Bacon's confidence in the fact that scientific and technological progress is a humanistic or humanitarian one was also supported by the idea of cultivating ethically neutral knowledge and moral responsibility for its application that could possibly harm people. The task of Bacon's programme of scientific development was to convince the great men of the world that financial and organisational support of science was necessary and useful for society and the state. This programme aimed at «arranging science as an intensive enterprise and institutionalising it socially so that its inventions could serve the man's well-being» [Böhme 1992]. This is the very main goal of *New Organon* and social Utopia *New Atlantis* by Francis Bacon. Multiplication of the man's power, establishment of the man's domination over nature, all useful kinds of art, manufacture, mechanisms and machines with the help of experiments, paying no attention to theology, ethics, politics, metaphysics, grammar, rhetoric and logic – that was the motto of the London Royal Society. This separation of natural science research from all ethical and religious matters that had a progressive character at that time is coming now to antagonism with modern social development because it blurs the limits of the possible for an individual and humanity in general, placing the former alongside of God the Creator as he produces Heaven on the Earth with the help of indus-



try, technology and science. In 1812 Sergey Bulgakov in *Philosophy of Economy* exclaimed with bitterness and suspense: Our generation seized up with this passion to a greater extend is loosing its loosing all limits to define the possible. «The world is plastic», it can be reconstructed and even reconstructed in various ways. We live under the impression of the more and more increasing might of our economy that opens boundless vistas for «cultural creativity» [Bulgakov 1990].

It is only through the connection between science, technology and economy that the slogan *Knowledge is Power* can be realised. This connection, on the one hand, leads to an instrumentalisation of knowledge, and on the other hand, to a growing dependence of even «pure» science on technology and economy. Man is placed in the centre of the world, his economic activity being interpreted as «a new force of nature, a new world-transforming factor that fundamentally differs from the other forces of Nature». Technology, according to Bulgakov, is «a combination of possible methods of man's impact on Nature for definite purposes set in advance». The very possibility of technology comes from the actual accessibility of nature for man's impact. Nature is treated as a passive source while man is an active, conscious source and in this sense he becomes the centre of the Universe, subordinating the rest of Nature to himself. «His potential world domain gets partly and gradually realised through the economic process». But the Man does not equal God, he «does not have omnipotence, ability to create everything he wants out of nothing». Man can act freely and originally only when he deals with the methods to use his own nature, his own nature as well as environment being given to him [Bulgakov 1990, 46-47, 62].

If ancient society set science a task to cognise that man can cognise, then Bacon sets a task to achieve man's domination over nature. This domination means that humanity with the help of exact knowledge of natural causes can use nature for some personal ends. By doing this, humanity would like to enjoy the rights to utilise nature, which was given by God. Man's domination over the material world is based, as Bacon sees it, totally on science and art. The danger may arise, however, of scientific and artistic results being placed at the service of vice and luxury or something of the kind, but it does not seem to Bacon too perilous because it cannot inspire anyone. Moreover, he believes that unlike political activity that aims at improving the state of affairs practically through the use of force and injustice, inventive activity can bring happiness and wealth without doing anybody harm.

Distinguishing three types of ambition that science could serve: (1) to multiply personal power in your native country, (2) to multiply the might of your native country and to make it dominate over other peoples and (3) to broaden the domination of human society over nature as a whole; Frances Bacon stresses that the latter is undoubtedly the healthiest and the noblest.

Trusting professional ethics is not enough from the present-day point of view. However, he does not discuss the effects of such applications of scientific and technological achievements for personal and political ends that do people harm. In his social Utopia *New Atlantis*, he speaks on the contrary, about the necessity of keeping these achievements as national secrets. The strict antagonism between man and nature, rare before Bacon but well established after him, is also problematic.

Science is to investigate the forces hidden in nature and enlarge as much as possible man's power over nature that is interpreted as a giant workshop for human activity. *New Organon* subserves this task as it deals with the logic of invention, the methodology of inventive activity that fundamentally transforms the world, for example, the invention of gun-powder or the compass. The application of a single invention inspires many people to consider the inventor a superman. But Bacon believes the discovery of a method that could facilitate further inventions deserves even greater respect. This method should throw light on things as they are, without superstition and deception, errors and confusion, which is worth more than the fruits of inventive activity altogether. Thus, Bacon changes the very system of human knowledge that is no longer treated as a closed system, a canon, but as a constantly renewable open system, a result of collective cognition. Science should in the future become a science of activity while its methodology should be based on a combination of empirical and rational abilities of the spirit. The methodology of research is here not a means of knowledge organisation but the transference of collective experience into underdiscovered fields of science. From here comes Bacon's concept of *scientific and technological process as a scientific experience passed over from generation to generation* and obtained at every moment of time as a result of co-operation of separated labour of researchers.

For the first time Bacon considers science to be scientific research, organised into research laboratories according to application spheres, meeting some social needs, i.e. serving these social needs directly. However, these are the needs, above all, of the national state, including scientific and technological development in the military sphere. As we can see, Francis Bacon's programme articulates and develops an aggressive approach towards the utilisation of natural resources for the ends of human society. The programme elaborated, being undoubtedly progressive at that time and having some underwater stones, was successfully implemented in the 19th – 20th centuries, but at the end of the 20th century we have come to the conclusion that this programme has exhausted itself completely [Böhme 1992].

Such super optimism concerning science and technology was given its final shape in the 19th century. Even *Renan*, a deeply religious Christian scientist for exam-

ple, says in one of his earliest books, *The Future of Science* (written in 1848–1849 under the impression of the French Revolution but not published until 1890), that scientific belief is a supreme derivation from Christian thinking and tradition [Wagner 1970]. From his point of view, science has the powers of both revelation and creation. Since its task is to organise people and God Himself, it needs full autonomy and boundless freedom. In this case the researcher becomes an authority for himself, free from any control. Thanks to science man, who is also the embodiment of the Spirit, achieves domination over matter. Such domination, as Renan expects, can be achieved as a result of scientific research, possibly, in a million years when human society perceives the laws of life and the atom and, by transforming elements and altering species, gains boundless power and control over the Universe. Scientific knowledge will become a real basis of ‘intellectual elite’ power that with the help of ‘preventive terror’ will save everything on the Earth from destruction and let the elite approach God, as they become super human. If the secrets of life can be discovered only at the sacrifice of humanity itself to build up a new world, it will mean that the predestination of human existence has already been achieved, i.e. (that is) man, grown up in the process of evolution from the animal kingdom, has mutated into the divine matter. Two decades later under the influence of the results of scientific and technological development, which can serve vice as well as virtue and whose consequences cannot be foreseen in the predictable future, Renan realised that by doing this man can break all possible limits. In the preface to his book Renan admitted that the expectations of boundless happiness which human society might achieve with the help of scientific and technological progress was purely an illusion.

In the same way P.K. Engelmeier, a Russian engineer and philosopher of technology, begins his booklet ‘Technological Results of the 19th Century’ with the words full of optimism: ‘Our 19th, technological, century is coming to an end, the century of steam and electricity, the century of unprecedented conquest of forces of nature’. Then, describing the achievements of technological progress, he writes: ‘Technology has conquered for us space and time, matter and power, being the power itself that irrepressibly turns the wheel of progress’ [Engelmeier 1898, p. 6]. Giving a rather optimistic assessment of the achievements, Engelmeier believes that the technological outlook was dominating in the 19th century not because of wide development of manufacture, railways, steamers, telegraph and other formal signs of the technological century, but also because of an inward tendency of Western European culture to overcome actual obstacles with actual power. Summing up the results of technological progress, Engelmeier mentions that for many thousands of years technology has been acting as an unconscious power unconsciously coming into a single combat with the elemental forces of nature. In the 18th century technology was recognised, called by its name and

placed alongside other noble and free professions [Engelmeier 1898]. *The main scientific feature of technology in the 19th century was to conquer the power of nature.* The function of science is to predict facts while the function of technology is to influence nature, evoking by artificial methods the desirable facts and to retard the undesirable ones. The technological outlook regards the world as a game of the forces accessible for our understanding and our impact on them, in other words, it plaites the will of man into other natural forces that govern the order of phenomena. To put it in a short phrase, the technological outlook is the 'Man is the architect of his own fortune' formula [Engelmeier 1900]. Man has learned to guide life according to his own desires. Engelmeier calls this skill technology. The genius of humanity over the past two centuries has surrounded us with the man-made microcosm within the natural one, because man should have done something to have his requirements satisfied, this something being expedient reforms of his living conditions. Which is why Engelmeier grants the leading part in society to *engineers who should become the technological elite of society*, on whose purpose the system of engineers' training should be improved. The emergence of technocracy in the 20th century showed how 'efficient' this management of society can be. It was rather difficult for Engelmeier as well as for Renan to foresee to what uncontrolled consequences this boundless scientific and technological progress might lead, especially in the military sphere.

In the USA, we already find as an objective in the foreground a task in «bionanotechnology» to make an ideal soldier ("Soldier Nanotechnologies") with extension of human sensory abilities and expanding brain functions through technical aids [The National Nanotechnology Initiative Strategic Plan 2007]. "Nanotechnology, in combination with biotechnology and medicine, opens perspectives for fundamentally altering and rebuilding the human body. At present, research is being done on tissue and organ substitution, which could be realized with the help of the nano- and stem cell technologies. Nanoimplants would be able to restore human sensory functions or to complement them, but they would also be able to influence the central nervous system. While the examples of medical applications of nanotechnology cited remain within a certain traditional framework – because the purpose consists of "healing" and "repairing" deviations from an ideal condition of health, which is a classical medical goal –, chances (or risks) of a remodelling and "improvement" of the human body are opened up. This could mean extending human physical capabilities, e.g., to new sensory functions (for example, broadening the electromagnetic spectrum the eye is able to perceive). It could, however, also – by means of the direct connection of mechanical systems with the human brain – give rise to completely new interfaces between man and machine, with completely unforeseeable consequences. Even completely technical organs and parts of the body (or even entire bodies) are be-

ing discussed, which, in comparison with biological organisms, are supposed to have advantages such as – perhaps – increased stability against external influences” [Grunwald 2005].

We mentioned ethical problems which originate today even more in connection with the extended power of humans to encroach in non-human environments, on “nature”. This would be valid especially as regards the possibility of new manipulations and encroachments on the genetic basis of life, the hereditary structures figuring in the genes. There is also a problem of the neurosensory men-machine interface that is a question of the compatibility of the damaged bio(natural) system and introduced implant (artificial system). A problem of sensoric-neuroelectronic interfaces would occur, if implants are inserted in an injured or partially damaged biological system. An injury within the central nervous system may hardly be healed or regenerate in a natural way. On the contrary, generally additional parts of the injured biological system will also degenerate or deteriorate. Nevertheless, due to the extreme manipulative capabilities of human encroachments there develops a rather or even totally a new ethical situation of the orientation towards humanitarianism. This requires new behaviour rules and possibly even a new ethics in a stricter sense. The future of “nature” and of human life seems to be in danger or at risk.

Trying to channel this rather “wild” expansion and growth of the rampant *technoscience super-structure* and its technological development and *systems technocracies* would indeed require a sort of revival or resuscitation of apparently old-fashioned virtues of *reason* in such domains as philosophy, humanitarianism, social responsibility and technology assessment. To note, the instigating effect of military developments and research for and in technology and the applied sciences is still going strong: R & D lead the way – mostly, indeed, in the form of military research and development, even frequently in so-called “pure basic research”. The problem of the technology assessment in the nanotechnology become complicated because there is no developed scientific community and therefore are no any experts in nanoscience and technology. «... we need to distinguish the loose everyday sense of ‘an expert’ — which can mean no more than an individual who knows a lot about a topic — from a more specific sense of the term, which is used when we are discussing the social role that experts should play. There are four features of expertise important to this social role that should be made explicit: 1) The expert has specialized training and knowledge not easily available to a layperson; 2) this knowledge is usually technical (this means at least the knowledge which is of specific methods for knowing or doing things); 3) the expert is recognized as such by his/her own professional community; 4) the professional community is recognized as legitimate within the larger society. While the first and second feature apply unproblematically to nanoscitech, the third and fourth

are more complicated» [Sanchez 2005]. In this case one of the key role in nanotechnoscience play the philosophical reflexions from the interdisciplinary and transdisciplinary point of view. We have to *reinstall philosophy*, in a rather modern and *up-to-date*, primarily future-bound form and fashion and *cross-disciplinary* combination. We have to develop, if not reinvent, a *practice-oriented* philosophy of technology, planning, risk assessments, responsible decision making, globalisation, etc. combined with notable perspectives for a human and humane future orientation, the creative designing of new ways and strategies to confront the mentioned overriding problems of social over-flooding and to develop a kind of rather optimistic activism, achievement-orientation and socially responsible normative stance in all our institutions of education and, beyond that, in our social and political as well as all-too-human lives.

Bulgakov emphasises that the theory of technological progress was transformed in the 20<sup>th</sup> century into a kind of progress theology that foretold the achievable with the help of modern technology future of the happy, proud and free man. To bring happiness to as many people as possible was put forward as a goal of that super modern religion where human society equipped with technological knowledge played the role of God [Bulgakov 1990]. That interpretation of progress comes close to philosophy of technology by Fred Bon, according to which the question 'What should I do to be happy?' is the most important question of technology [Bon 1898]. The first Russian philosopher of technology, P.K. Engelmeyer, who also came from the initial premise of Bon, deemed the significance of technology in modern culture to have an eudemonical approach: "Man is a hammer-man of his happiness". These words express so called technological optimism of the first philosophers of technology. "Technological optimism is more evident in the statements that treated technological process as the cause of cultural progress in general or just identified with the progress itself... The extreme form of technological optimism was characterised by specific euphoric expectations of the future» when Humanity will be able to reach material but not cultural Heaven on the Earth and even obtain cosmic power" [Van de Pot 1995].

However, Fred Bon as well as Engelmeyer consider this goal of achieving Happiness to be subordinated under a higher idea of achieving Virtue. "Technology is an application of our life knowledge to life itself, i.e. on the one hand, to maintaining of life (protection), on the other hand – to expanding of life (aggression). All that hinders life is vice and harm, all that promotes life is virtue and use. Technology is a means to fight against Harm and its conversion into Use". Ethics deals with the matter of Virtue whereas technology deals with the matter of Use. "As the goals of Virtue and Use interrelate, or as they sometimes differ, ethics and technology may interrelate or differ", respectively [Bon 1898]. Speaking about the eudemonical ideal S. Bulgakov mentions that this ideal, if taken as a scale

for the assessment of historical development, inevitably leads to immoral consequences. Technology begins to dominate over Man, not to serve him, and makes him not happy (as, for example, Engelmeyer thought) but miserable.

According to Bulgakov, first, the eudemonical ideal leads to an idealisation of human requirements, second, this idea treats the sufferings of one generation of people as a bridge to the happiness of the next generations. It makes no difference among to the concept if these are of the sufferings of the present generation to achieve happiness of their children and grandchildren (according to Dostoyevsky, to manure future harmony by personal sufferings), as the communist ideas promised, or, on the contrary, happiness of the present generation is achieved at the expense of the destroyed life space for all generations to come, if we speak about squandering of natural resources and contamination of environment. It is well-timed to remember Dostoyevsky saying that to build your own happiness upon unhappiness of the others is an immoral thing. The first and the main task that theory of progress sets itself is to show that History has sense and the historical process is not only evolution but progress as well. This task is too heavy for empirical science as it has a metaphysical character. The absolute law of Virtue that should become the law of our life "when applied to historical development tells us to mean well in history and do our best to promote the realisation of Virtue, tells us, in other words, to mean progress. Progress is, from this point of view, a moral task, not existence, but the absolute imperative." [Bulgakov 1990]. The energy transmitted by huge machines rendering amounts of energy not available before and multiplied by the technological power of man regarding interference and change executed by humans over nonhuman environment, over nature and especially the availability of interventions and even nanomachines will lead to extraordinary challenges for the mentioned "future ethics". From the immensely grown capabilities of technological impacts totally new situations for ethical orientation will occur not only regarding behaviour rules but also pertaining to responsibility and provision as well as providence and caring for the future. This would require new norms, in part changed values and frames of reference: this is beyond any doubt a totally new situation in the history of humankind: humans had never before had such power to destroy or decisively harm all or some life in a specific ecological system or even on a global scale by using their technological interventions and interferences as well as encroachments on these natural entities. Ethics would gain a new humanistic relevance not only ecologically speaking but also as a new future-oriented ethics of responsibility.

As we can see, the situation in the 20<sup>th</sup> century has changed. "We cannot hope for omnipotence of Nature any longer. The natural mechanisms are not sufficient at present to preserve the biosphere. New methods for regulations, based on the understanding of natural processes and to some degree of the managing such proc-

esses, are required. The anthropogenic regulation is the forecast of natural cataclysms and punctual decrease in speed of the process. It is the choice between the immediate profit and long-term revenues in the usage of natural resources" [Marfenin 2000] and mankind.

Making reference to Renan, Berdiayev warns that technology can provide man, even a small group of people with a great destructive power. "*Soon peaceful scientists will be able to produce upheavals of historic and cosmic character*". This leads to the concentration of power in the hands of those who possess technological secrets. The future of all humanity depends on this. In Berdiayev's opinion, «the technological epoch», the epoch when technology dominates over the human soul, will inevitably end in victory of the human spirit, not in negation of technology, but in its subordination to the human spirit and spiritual values of life. Technological civilisation, society of technology and machines want man to be their part, deprived of personality. "Technology would perpetrate a deadly punch to the humanistic ideal of Man and culture. The machine is essentially anti-humanistic." Technology is always merciless to the living stock, but it is mercy to all the living and existing stock that should restrict the power of technology in our life [Berdjajew 1949]. „Mighty strides in physics have been characteristic of our era. Within physics there is occurring a genuine revolution. But the discoveries, which the physics of our era is uncovering, are characteristic of the decline of a culture. Entropy, connected with the Second Law of Thermodynamics, radioactivity and *the decaying apart of atoms of matter*, the Law of Relativity – all this tends to shake the solidity and stability of the physico-mathematical world-perception, and it undermines faith in the lasting existence of our world. I might say, that all this – represents a *physical apocalypse*, a teaching about the inevitability of the physical end of the world, the death of the world" [Berdyayev 1992]. In the relation to nanotechnology we may today speak about Nano-Armageddon or apocalyptic(al) nanoethics. „The recent excitement about nanotechnology is only the latest offspring that comes in the bizarre form of apocalyptic ethics, propagated particularly by influential transhumanists" [Schummer 2006].

Indeed, overriding multi-disciplinary knowledge and information are and have to be used almost everywhere (any large-scale practical problem whatsoever is multidisciplinary!) on the one hand, and we are, on the other, bound to a human, humane, humanitarian, and ecological perspective, i.e. as regards the latter one of sustainability and sustainable development, that have to be taken into account in all essential social and political realms leading beyond the mere addition of information, extension and scope of networks as well as the ever faster breaking waves of innovations in technologies and applied sciences to be implemented for economic, military and industrial practice. Many people even talked about "the military-industrial complex" having undergone a mutation towards an "econom-



ic-industrial-technological-scientific complex” of technoscience bearing the characteristics of a real super-structure impregnating all areas and walks of life. That is to say nanoethics has to combined scientific, technological or engineering and economy ethics.

It would distinguish the human being most specifically that it should bear responsibilities and duties not only for its own actions but also for and as regards other living entities of nature and natural systems. As such a distinguished part of the totality of nature, as a specifically powerful agent (s)he has to take over a representative responsibility for “the total” in relationship and proportion of his technological power. This is true also morally speaking. It is indeed specifically human and a characteristic of part of their special position and dignity that humans may and have to attribute to other beings and kinds some “right” of existence and preservation, quasi-rights so to speak. That means that they have to take over duties of protection towards them *without reciprocity*. This applies to the total system as well as the larger systems of nature, since the human being is the knowing being who is able to go beyond its anthropocentric purview lending a (quasi) right of existence to other living beings. This overall ethics of *stewardship* seems to be more dignified and humane than the traditional self-limitation on human interests and comprehensive domination. This should be an insight not only in economical, ecological, informational, technological ethics but also for nanoethics.

## References

- Baumgartner C. (2006), Nanotechnologie in der Medizin als Gegenstand ethischer Reflexion: Problemfelder, Herausforderungen; Implikationen, Nordmann, A., Schummer, J., Schwarz, A. (Hrsg.) Nanotechnologien im Kontext, Akademische Verlagsgesellschaft, Berlin
- Berdjajew N. (1949), Der Mensch und der Technik. Cornelsen Verlag, Berlin-Bielefeld
- Berdyaev N.A. (1922), The Pre-Death Thoughts of Faust, Bereg, Moscow, online at [http://www.berdyaev.com/berdiaev/berd\\_lib/1922\\_059.html](http://www.berdyaev.com/berdiaev/berd_lib/1922_059.html)
- Böhme G. (1992), Am Ende des Beconschen Zeitalters, Wissenschaft und Gesellschaft, 3
- Bon F. (1898), Über das Sollen und das Gute. Eine begriffsanalytische Untersuchung, Verlag von Wilhelm Engelmann, Leipzig
- Bulgakov S. (2000), Philosophy of Economy, New Haven and London, Yale University Press

- Bulgakov S.N. (1990), *Philosophy of Economy*. NAUKA, Moscow (in Russian)
- Engelmeyer P.K. (1900) *Philosophie der Technik, eine neue Forschungsrichtung*, Prometheus, 1900, 564, 659-692
- Engelmeyer P.K. (1898), *Technological Results of the 19<sup>th</sup> Century*, St. Petersburg (in Russian)
- Grunwald A. (2008), *Nanoparticles: Risk Management and the Precautionary Principle, Emerging Conceptual, Ethical and Policy Issues in Bionanotechnology*, Springer, Frankfurt a.M., 85-102
- Grunwald, A. (2005), *Nanotechnology – A New Field of Ethical Inquiry?* Sci. Eng. Ethics, 11, 2, 187-201
- Lenk H. (1994), *Macht und Machbarkeit der Technik*, Stuttgart: Reclam
- Lenk H. (2003), *Der Mensch im Spannungsfeld von Natur und Technik: Die neue Verantwortung für unsere Umwelt und Zukunft*, Jahrbuch des Deutsch-Russisches Kollegs 2001-2002, Hrsg. Von V. Gorokhov, Aachen: Shaker Verlag, 26-39
- Lenk H., and Maring M. (2001), *Responsibility and Technology, Responsibility. The many faces of a social phenomenon*, L., N.Y., Routledge
- Marfenin N.N. (2000), *Ecology and Humanism, State of Russia in the Surrounding World: 2000*, IIUEPS Press, Moscow, 41-42
- Mitcham C., and Duval R.S. (2000), *Engineering Ethics*, Prentice Hall, Upper Saddle River, NJ
- Müller S. (2006), *Minimal-invasive und nanoskalige Therapien von Gehirnerkrankungen: eine medizinethische Diskussion*, Nordmann, A., Schummer, J., Schwarz, A. (Hrsg.) *Nanotechnologien im Kontext*, Akademische Verlagsgesellschaft, Berlin
- Nanotechnologie erobert Märkte* (2004), *Deutsche Zukunftsoffensive für Nanotechnologie*, BMBF, VDI, Bonn, Berlin
- NewScientistTech (2007), NewScientist.com news service, online at <http://technology.newscientist.com/article/dn12358-fda-finds-no-proof-of-harm-with-nanotech-products.html> / accessed 26 July 2007
- Sanchez N.E. (2005), *The Experts Role in Nanoscience and Technology*, Baird, D. et al. (eds) *Discovering the Nanoscale*, IOS Press, Amsterdam, 261-262
- Schummer J. (2006), *Cultural diversity in nanotechnology ethics*, Interdisc. Sci. Rev., 31, 3

Schwanke Ch. (1994), (Hrsg.), Ethik in Wissenschaft und Technik. Erfahrungen und Perspektiven im interdisziplinären Dialog, Forum Humane Technikgestaltung Friedrich Ebert Stiftung, Bonn, Heft 11

The National Nanotechnology Initiative Strategic Plan (2007), National Science and Technology Council, Washington, online at [http://www.nano.gov/NNI\\_Strategic\\_Plan\\_2007.pdf](http://www.nano.gov/NNI_Strategic_Plan_2007.pdf) / accessed 20 December 2007

Van der Pot J.Y.J. (1985), Die Bewertung des technischen Fortschritts: eine systematische Übersicht der Theorien, Van Gorcum & Comp. Assen, Maastricht

Wagner Fr. (1970), Weg und Abweg der Naturwissenschaft. Denk- und Strukturformen, Fortschrittsglaube und Wissenschaftsreligion, München: C.H. Beck

What is Nanotechnology? (2008), Center for Responsible Nanotechnology. <http://crnano.org/whatis.htm> / accessed 2008

# Regulation models addressing data protection issues in the EU concerning RFID technology

---

---

Ioannis Iglezakis

---

---

## 1. Introduction

Radio frequency identification (RFID) is a new technology that is destined to change our lives in many areas, such as logistics, healthcare, public transport, the retail trade, etc., as it provides new business opportunities, cost reduction and increased efficiency (Commission, 2009). RFID uses radio waves for the automatic identification of individual items and thus, it allows the processing of data over short distances (Bannon, 2008). In more particular, RFID systems are considered as the next generation of bar codes, offering much more advantages, since they identify uniquely objects which bear a RFID tag, without line-of-sight contact, and allow for wireless transmission of data and connecting to databases and applications (A. Juels, 2006).

The main components of an RFID infrastructure are a tag and a reader. The tag on the one hand consists of an electronic circuit that stores data and an antenna which transmits the data, while the reader on the other hand has an antenna which receives the data and a demodulator which translates the analogue information into digital data (Article 29 Working Party, 2005, p. 3). The RFID reader sends and receives back signals from the tags via one or more antennas and transmits the data to databases or software applications.

An RFID tag can be easily embedded onto various products, their packages or even be implanted beneath the skin of a human (Talidou, 2006). The size of the RFID tag, which is particularly small, about 0,4 mm<sup>2</sup>, is an important factor for its proliferation.

A common taxonomy of RFID systems makes a distinction between passive tags, i.e. those tags that have no own power supply and receive energy from the reader antenna, and active tags, i.e. those tags that have their own power supply. Passive RFIDs are very small and inexpensive and their life span is almost unlimited and this makes them ideal for tracking materials through supply chains (R. Levary et al., 2005). Active tags are more powerful, as they can emit the stored data, rewrite those data and store new data. However, their life cycle is shorter. Since they present more possibilities of data processing they are considered more privacy intrusive (Synodinou, 2009).

The applications of RFID technology are extended in many sectors. The retail sector was one of the first to adopt this technology, which provides the retailer the possibility to control and lever the availability of products in a store and in storage. It also makes possible product traceability and recall of faulty or unsafe products, etc. It makes, therefore, no surprise that an unprecedented growth in sales of passive EPC RFID tags took place in 2010 and that the sales volume exceeded one billion units<sup>1</sup>, while prices of tags also are decreasing.<sup>2</sup>

In transportation and logistics, the said systems are implemented in order to track vehicles and products, providing security during transport. Particularly, high is the importance of this technology with regard to public transportation and as far as electronic toll collection and access to public transportation (e.g., e-ticket) are concerned (Talidou, *op.cit.*).

Furthermore, of great importance is RFID technology in healthcare, where it is implemented to make tracking of medicines easier and prevent counterfeiting and loss derived from theft during transportation. It would also enable pharmacists or stores selling medicines to verify the origin of medicine. In hospitals such systems may be used, e.g., to eliminate the risk of leaving items inside a patient after an operation and to locate track personnel in case of emergency, while RFID tags may be attached to patients so that it would be easier for the personnel to treat them (WP, *op. cit.*, p. 4).

Other applications of RFID are implemented for security and access control, e.g., to monitor valuable equipment or as components in a car immobilizer system, in aviation for baggage handling purposes, in libraries as a replacement of electromagnetic and bar code systems of control, for the tracking animals, but also for the tracking of people. It is notable that a club in Barcelona offered its clients a RFID microchip that had to be implanted in their arms, which would gave them access to VIP lounges and could also be used for billing. Last, but not least, RFID chips are used in passports and identity cards, as they provide enhanced security as regards identification of individuals.

- 
1. See RFID Journal, Sales of EPC RFID Tags, ICs Reach Record Levels, available at: <http://www.rfidjournal.com/article/view/7952>.
  2. Notably, the price of a 96-bit EPC inlay costs from \$0.07 to \$0.15, whereas if the tag is embedded in a thermal transfer label on which companies can print a bar code, the price is \$0.15 and more, and low-and high-frequency tags tend to cost more. RFID readers, on the other hand, cost from \$500 to \$2,000; see RFID Journal, FAQs, available at: <http://www.rfidjournal.com/faq/20>.

## 2. The risks to privacy

An invasion to informational privacy might occur in case personal data are being processed by automatic or traditional methods. The sole requirement for the respective data protection rules to apply is that information undergoing processing is qualified as personal data, i.e. as information relating to an identified or identifiable natural person, in the sense of the Data Protection Directive.<sup>3</sup> For RFID systems to underlie the provisions of a data protection act it is, thus, required that RFID information are directly or indirectly referred to a natural person (WP, *op. cit.*, p. 8).<sup>4</sup>

This is the case, at first hand, where RFID systems are implemented in order to collect information directly or indirectly linked to personal data, so e.g., where products from a store are tagged with unique product codes which the retailer combines with customer names collected upon payment with credit cards and link them with the customer database. It is also the case where personal data is stored in RFID tags, so, e.g. in transport ticketing. And finally, RFID systems may be used to track individuals without a direct link to a natural person. It may happen, e.g., that a store provides cards with RFID tags to its customers and then monitor their shopping habits and make use of relevant data for marketing purposes. Even if the customer is not directly identified by means of the tagged card, he can be identified each time he visits the same shop as the holder of the card. Similarly, an individual can be tracked by shops which scan tagged products of customers. And further, third parties may use readers to detect tagged items of by passers, violating in that way their privacy (WP, *op. cit.*, p. 6-7).

As it is obvious from the aforementioned examples, RFID technology provides the potential for tracking and profiling of individuals. Due to the fact that RFID tags can be read without line-of-sight and from a distance without being noticed, they are prone for application by retailers for customer profiling, as well as for monitoring for other purposes, e.g., for law enforcement purposes, etc. Such practices are infringing, however, the right to privacy of individuals, as they are not complying with basic principles of data protection legislation.

Besides that there are also security threats arising from the fact that RFID tags can be secretly read, particularly in case they are hidden inside product packaging or other items and devices, and since RFID readers can also be concealed

---

3. Article 2 lit. a of Directive 95/46/EEC, L 281, 23/11/1995.

4. See, e.g., Weinberg (2007), who points out that: 'It would be a mistake to conclude that an RFID implementation will pose no meaningful privacy threat because a tag does not directly store personally identifiable information, instead containing only a pointer to information contained in a separate database.'

(Ayoade, 2007, p. 558). Security issues arise for businesses, referring to espionage, unauthorized access of competitors to customers' preferences and security attacks (DoS, etc.). Personal privacy threats are more important, since individuals are exposed to the risk of their behavior being covertly monitored (Garfinkel et al., 2005).

### **3. Compliance with legal requirements of data protection**

#### **3.1 Directive 1995/46**

The Article 29 Data Protection Working Party in working document of January 19, 2005 stresses out those data controllers which implement RFID systems must comply with the obligations of the data protection Directive (WP, op. cit., p. 5 et seq.). Accordingly, the principles related to data quality must be observed, i.e., the use limitation, data quality and conservation principles. Thus, any further processing of data, which is incompatible with the purposes of collection, is prohibited, further that irrelevant personal data must not be collected and data must be kept for no longer than it is necessary for the purpose of collection or processing.

What is more important is that data processing must be based on one of the grounds of legitimization foreseen in Article 7 of the Directive. Thus, data processing will be based in most cases on consent of the data subject, as the other requirements are not fulfilled, with the exception of the case where processing is necessary in order to protect the vital interests of the data subject, e.g. where RFID technology is used in the health sector to track items used in surgical operations or to identify and provide treatment to patients. Wherever RFID systems are implemented, e.g., by stores that offer loyalty cards to their customers should require consent from their customers to collect and process their personal data, since this would go beyond the scope of the contract.

Where RFID systems are used by corporations and stores to track products to prevent theft etc., it is appropriate to examine whether processing is necessary for the purposes of legitimate interests pursued by the controller. In our view, this requirement is not fulfilled, if tags do not incorporate privacy features, such as the "kill" command, i.e. the possibility to permanently or temporarily deactivate the tag, or the blocking of a tag (Ayoade, op. cit., p. 559). Other technical solutions that have been proposed are i) the use of encryption on tags and ii) the inclusion of a privacy bit, i.e. a logical bit resident in the memory of an RFID tag indicating the privacy properties of the tag (Talidou, op. cit., p. 14).

The Working Party also emphasizes that data controllers that use RFID systems must fulfill the information requirements, guarantee the data subject's right of access and implement appropriate technical and organizational measures. Par-

ticularly, as regards the right of information, it is underlined that a retailer shop which employs RFID technology must provide data subjects at least with clear notice about following information: a) the presence of RFID tags on products or their package and the presence of readers, b) whether the presence of such devices enables the tags to broadcast information without individual engaging in any active action, c) the purposes for which the information is used and iv) the identity of the controller. Furthermore, data controllers must inform individuals how to discard, disable or remove tags from products and how to exercise the right of access.

However, here lies a difficulty: how can the owner of a tagged item determine what information is on the tag, who processes the stored data and for which purposes? (Flint, 2006). Due to the technical characteristics of RFID tags the right of information seems hardly realizable and only with increased cost of the tag (Garfinkel et al., 2005).

### **3.2 Directive 2002/58**

The provisions of Directive 2002/58 on privacy in electronic communications apply also to RFID systems, particularly as this was amended by Directive 2009/1365, which re-defined the field of application of the former Directive. It applies thus "to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices".

Consequently, data controllers must comply with those provisions of the Directive which are relevant in case of data processing in RFID systems. In accordance with Article 5 (3), the storing of information or the gaining of access to information stored in the terminal equipment of a user, i.e. in an RFID tag, is only allowed if the user has given his consent, or if it is necessary for the provision of an information society service. The latter condition is not fulfilled in the context of RFID systems and therefore, consent to write data or gain access to data in RFID tags is compulsory.

The consent of the user is also necessary condition for the use of RFID technology for the purposes of direct marketing, pursuant to Article 13 of the Directive.

Furthermore, data stored in RFID tags can be regarded as location data, in the sense of Article 2 lit. c of the Directive, i.e. as data indicating the geographic position of the terminal equipment of a user. This is particular significant, since users can be located and their associations can be tracked (Talidou). Article 9 of

---

5. See Recital Nr. 56 of Directive 2009/136.



the Directive provides for that users' or subscribers' consent must be given for the processing, as well as that they must be informed about the details of the processing before they provide their consent.

However, the field of application of this Directive is restricted only to processing taking place in public communications networks and thus, RFID applications which do not use such a network are exempted.

### ***3.3 A Privacy and Data Protection Impact Assessment Framework***

The European Commission issued a recommendation of May 12, 2009, in which it elaborated on self-regulation mechanisms and in particular, on the development of a framework for privacy and data protection impact assessment (Recommendation, 2009). In this recommendation it invites EU Member States to ensure that the industry in collaboration with relevant civil society develops a framework for privacy and data protection impact assessment (PIA), which would be submitted for endorsement to the Art. 29 Working Party.

It also calls Member States to identify applications posing information security threats and develop a concise, accurate and comprehensible information policy for RFID applications. It provides that operators must inform individuals of the presence of tags, using a common European sign developed by European Standardisation Organizations. And it goes even further, as it provides that retailers should deactivate or remove at the point of sale tags used in their application unless consumers give their consent to keep tags operational (Commission, op. cit., Nr. 11). This obligation may not apply, in case an impact assessment concludes that tags which used in a retail application and remain operational after the point of sale do not represent a likely threat to privacy.

Subsequently, an informal workgroup led by industry representatives delivered on March 31st 2010, a PIA of RFID applications, in cooperation with stakeholders including consumer groups, standardization bodies, and university scholars.<sup>6</sup> The Working Party was critical and did not endorse the proposed the proposed Framework. It laid down its objection in Opinion 5/2010, in which it invited the industry to propose a revised privacy and data protection impact assessment framework. ENISA also published an opinion, making recommendations to improve the proposed PIA.<sup>7</sup> Next, the industry redrafted a revised PIA framework

---

6. Industry Proposal on Privacy and Data Protection Impact Assessment Framework for RFID Applications of March 31 2010, available at: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175\\_annex\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_annex_en.pdf).

7. ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications of March 31, 2010, available at: <http://www.enisa.eu->

and this which was submitted for endorsement to the Article 29 Working Party on January 12, 2011.<sup>8</sup> The Working Party delivered an affirmative opinion, endorsing the Revised Framework.<sup>9</sup> In its opinion, the Working Party acknowledges that a PIA is a tool designed to promote “privacy by design”, better information to individuals as well as transparency and dialogue with competent authorities.

#### 4. Regulation vs Self-Regulation

It is indisputable that privacy issues related to RFID technology can not be solved by means of existing legislation alone and that tools other than regulation are necessary. Evidently, the provisions of the EU Data Protection Directive are too general, while the ones of the eCommunication Directive are restrictive as to their scope. In our view, there are two ways to solve this issue: one is to provide for mandatory PIA that would be made available to data protection authorities and the other alternative is to provide for mandatory technical solutions (privacy enhancing technologies) in RFID technology.

In more particular, although the existing Data Protection Directive contains rules that could be applied to data processing in RFID systems, its provisions are very general and in many cases it is unclear whether the processing includes personal data. The eCommunications Directive also contains interesting provisions, but it can only apply in processing taking place in public communications networks.

The PIA Framework that was endorsed by the Article 29 Working Party is an important instrument and its basic advantage is that it applies differently in each specific application, depending on the risk posed. It also provides for the documentation of System Protection and RFID Tag Protection, including access controls, policies on the retention and disposal of personal data, and technical measures such as encryption to ensure the confidentiality of the information, tamper resistance of the tag and deactivation or removal of the tag, if required or otherwise provided. However, the recommendation on which the PIA Framework was based is not mandatory, but it is drafted to provide guidance to EU Member States on the design and operation of RFID applications. Thus, the effects of the proposed measures remain unsure, as it is not certain whether Member States will implement this recommendation and in which way, if they will make it mandatory or introduce it as part of a code of conduct, etc.

---

[ropa.eu/media/news-items/enisa-opinion-on-pia](http://ropa.eu/media/news-items/enisa-opinion-on-pia).

8. Privacy and Data Protection Impact Assessment Framework for RFID Applications of 12 January 2011, available at: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180\\_annex\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf).

9. Data Protection Working Party, Opinion 9/2011, WP 180.

To effectively address the data protection issues posed by RFID technology another regulatory approach is needed. In particular, this will require making the PIA process mandatory, providing also for the notification of its results to the competent data protection authorities, which should have the right to prior checking of RFID systems posing significant privacy risks.

Alternatively, the data protection legislation could introduce specific rules for RFID systems and more particularly, rules establishing technical solutions, since it is difficult to achieve privacy by design by self-regulation. Such rules are already foreseen in the Framework PIA as mentioned above, but they would be more effective once included in mandatory rules.

## References

article 29 Data Protection Working Party. Working document on data protection issues related to RFID technology, WP 105, January 19, 2005, available at: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf)

Ayoade, J. 2007. Roadmap to solving security and privacy concerns in RFID systems, *Computer Law & Security Report* 23 (2007), pp. 555-561.

Bannon, A. (2008). RFID: Radio Frequency Identification OR Real Frailty in Data Protection?, *The Journal of Information, Law and Technology (JILT)*, available at: [http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2008\\_1/bannon](http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2008_1/bannon)

Commission Recommendation (2009). On the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C (2009), 3200 final.

Flint, D., 2006. RFID tags, security and the individual, *Computer Law & Security Report* 22, pp. 165-168.

Garfinkel, S., Juels, A., Pappu, R. (2005). RFID Privacy: an overview of problems and proposed solutions (Computer Society). *IEE Security and Privacy* May-June 2005, Issue 3, pp. 34-43.

Juels, A. (2006). RFID Security and Privacy: A Research Survey, *IEEE Journal on selected areas in Communications*, vol. 24., No. 2, February, available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.5249&rep=rep1&type=pdf>

Levary, R. Thompson, Kot., K., Brother, J. 2005. Radio Frequency Identification: Legal Aspects, 12 *RICH. J.L. & TECH.* 6 (2005), available at: <http://law.richmond.edu/jolt/v12i2/article6.pdf>

Synodinou, T., 2009. RFID Technology and its Impact on Privacy: Is Society One Step before the Disappearance of Personal Data Protection, in: Politis, D., Kozyris, P., Iglezakis, I., Socioeconomic and Legal Implications of Electronic Intrusion, pp. 89-107.

Talidou, Z., 2006. Radio Frequency Identification (RFID) and Data Protection Legal Issues, in: S. Paulus, N. Pohlmann, H. Reimer (Eds.), Securing Electronic Business Processes, Vieweg, pp. 3-16.

# Video games and the law

---

---

Philippe Jougoux

---

---

Video games have gone a long way since the first games of tennis on a green screen<sup>1</sup>. In USA only, 67% of households play video games<sup>2</sup> and the market is estimated to be around 10 billions of dollars. In Europe, the statistics are less important but still quite convincing of the phenomena, since 24% of the population is a “gamer”. The law of video and computer games, however, is still seen for most lawyers at best as a curiosity, at worse as a loss of time. The aim of this paper is to fight against these prejudices and to present the last developments of the law of video games.

Video game law is divided in three different sectors: the question of authorship of the creation, which includes application of copyright law but also of patent and trademark law, the new topic of virtual reality, which represents a fundamental transformation of the legal nature of the video game, from intangible goods to provisions of services, and the question of freedom of speech and its necessary balance with the legal protection of minors. This last part won't be analyzed in detail here as (even if it is sometimes discussed) video games do not present any specificity from a legal point of view, by comparison with other media. This position has recently been confirmed in USA by the Supreme Court in the case *Brown v. Ema*<sup>3</sup>. At issue is a California law banning the sale of such games to minors. The video-game industry argued that, unlike similar laws banning the sale of pornography to minors, the state's ban on video-game sales and rentals violates the First Amendment and asked for the law to be declared unconstitutional. The Supreme Court issued a 7-2 opinion striking the California law as unconstitutional and in other words decided to consider video game as an ordinary media, which should receive the same protection as TV, radio or the press.

---

1. The first video game in history was “tennis for two”, a two-dimensional, side view of a tennis court on an oscilloscope screen connected to controllers, on 1958. Source: <http://www.bnl.gov/bnlweb/history/higinbotham.asp>.

2. <http://www.esrb.org/about/video-game-industry-statistics.jsp>.

3. [supremecourt.gov](http://supremecourt.gov). 2011. Retrieved 2011-06-27.

We will then analyze distinctly the two other domains of the video game law and we will show that, in both cases, the technological development has completely modified the basic elements of the legal framework.

## **1. Video games and copyright law**

Video games are protected by copyright. In Europe and in America, the question is being discussed for a long time now, and it is actually possible to arrive to some conclusions about the legal nature of the video game. Also, copyright law does not only cover the games but also the consoles themselves. The modern consoles are in fact a type of personal computers with an operating system and the question of their protection involves huge economic interests.

### ***1.1. The video game, a very peculiar work of mind***

The scope of this paper is to adopt a comparative approach. A first difficulty emerging is to determine the conditions of protection of a work of mind by copyright law. In the continental author's right system, a work of mind has to be original in order to be protected, but in the common law copyright legal system, a work of mind needs additionally to be materialized on a support to fulfill the so called fixation requirement. In a video game, some pictures and models are already incorporated in the game, but the effects, the textures, the context are added at the moment of the execution of the video game. In the already classic decision *Midway Manufacturing Co. v. Artic International, Inc.* (1982) about the legal protection of the PacMan and Galaxian video game, Artic's defense to the accusation of infringement was that Midway's video games were not "fixed in any tangible medium of expression". Specifically, Artic claimed that the ROM chips in the Midway games never held pictures in any fixed medium, but rather contained instructions to generate pictures that were not themselves fixed. District Judge Bernard Decker ruled against Artic, noting that the law does not require a work to be written down in the exact way that it is perceived by the human eye. The judge was persuaded by Midway's demonstrations showing that the images in the games' demo repeated identically every time the games were turned on. The games also repeated in similar ways during subsequent plays.

So if a video game is original and it is fixed, it enters in the scope of protection of copyright law. This point has never really been discussed either in USA or in Europe. But what is protected exactly? Most of the video games are a complex assemblage of different components: pictures, video, music, scenario, software. The question is far to be rhetorical. For example, if the video game is deemed to be an audiovisual work, in Greece the legal framework of the collective work will probably apply, which grants the authorship of the work to the director. At the

opposite, if it is not a collective work, authorship of the work is shared between the plurality of the creators under the regime of joint authorship.

In 2003, the French Cour de Cassation rejected the idea that a multimedia is an audiovisual work, since at the opposite of a movie it incorporates an element of interactivity which constitutes the essence of the video game. The movie is constituted by a predetermined sequence of images, while in the video game the players choose the sequence of images by their actions<sup>4</sup>.

The interactivity is created by the software of the video game. If the interactivity is the fundamental part of the game<sup>5</sup>, does this mean that the video game is in fact just a software? The judges in the past were attracted by this idea<sup>6</sup>. For example, the Cour de Cassation in a decision of the 27th of April 2004 decided that “since the programming of an electronic game is not dissociable of the combination of sounds and pictures forming the different phases of the game, the analysis of the elements permits to determine the originality of the software”.

But the French judges have recently changed their mind in another interesting case. A company, which is a video game editor, created video games which incorporated some music. The company got bankrupt and the following simple problem was raised: could a collective management society representative of the right holders of music be present in the procedure? In other words, are the video games created by the company protected as software? If they are, according to the law, the right holders can just ask a lump sum, if not, they can pretend to a proportional remuneration.

The judges decided that “the video game is a complex work of mind which can’t be reduced to its only software dimension, independently of its importance, and then each of its component is ran by the legal framework that applies according to its nature”<sup>7</sup>.

The word is given: complex ! The reality of the work of mind that constitutes a video game can’t be considered just under the specter of one legal regime. The video game is by nature a work of collaboration and each author keeps copyright over his contribution. We have to recognize that this evolution for one time goes in the way of the practice. Nowadays, video games are divided in very specific

---

4. CourCass, 1<sup>ère</sup> ch.civ., 28 janvier 2003, C.c./Sté Havas interactive et Dalsace.

5. Irini Stamatoudi, Video game as a test case, p. 167, in Copyright and multimedia works, Cambridge, 2002.

6. See for example: CA Caen, 19 Déc. 1997 · CourCass, 21 juin 2000, affaire Pierre T. c/ Midway Manufacturing Company.

7. Cour de Cassation, 25 Juin 2009, arrêt Cryo .

units of production, whereas and for the 3D action games, most of the times the software itself, namely the 3D engine, is not a part of the game. The software companies rent 3D engine, software, that is used by the video game companies for their games. The fragmentation of the legal regime of the video game, while necessary, creates at the same time a lot of questions related to the way that the different sectors of protection could be juxtaposed and coordinated.

In France, the Law of the 5<sup>th</sup> of March, 2007 provides a legal definition of video games: it is a “software of leisure put in the disposition of the public on a tangible medium or online which incorporates elements of artistic or technological creation, and which proposes to one or more users a series of interactions based on a scripted framework or a simulated reality by the way of animated pictures, with or without sound”.

### ***1.2. The consoles software and the modchip problematic***

Video game industry lies primarily on the consoles' sales. The technological evolution has led to an increase of protection of video games, which takes various forms such as online activation schemes and DRM, but at the same time, the consoles, each day more like computers, have become vulnerable to manipulation. Microsoft, Sony and Nintendo started a global war against the modification of their consoles. We will analyze in more detail the situation of Sony, whose legal adventures have greatly influenced the evolution of information law. Of course, the phenomenon of globalization of the industry of entertainment leads to the conclusion that the same legal problems appear everywhere. But the Italian case law on this topic is very illustrative of the problem and deserves our attention.

The case is related to the popular console “Playstation 2”, which, as it has already been stated, is a real computer whose capacities have been locked by the constructor in order to limit its functionality to the execution of genuine video game for PS2 only. Because the consoles are sold below their cost, in order to attract new consumers, the practice permits to Sony to gain a substantial remuneration on the sale of the video games. Also, the lock of the machine offers to Sony the possibility to compartmentalize the market in 3 different geographical zones, according to the financial capacities of the consumers of the zone. We won't discuss the questions of competition law. The main issue is to determine the legal regime of the so-called mod chips, the devices created to unlock the functionalities of the console. Are they illegal and on which legal basis?

Article 6 of the Infosoc Directive 29/2001/EC expressly condemns the practice of circumvention of a technological measure of protection. However provisions which correspond to the same philosophy can be found in the American Digital Millenium Copyright Act (DMCA). Sony used the transposition of this article in



the Italian legal system to pursue the constructors of the mod chips. But according to the Court in the decision of 2003, the mod chip's main purpose was not to allow the loading of pirated copies, but to overcome monopolistic barriers and to exploit PlayStation functionalities at their best. The question is related also to the legal qualification of the video game: if the video game is a software, then the consumer is authorized to proceed to the creation of a backup copy and by consequence the mod chip finds a justification. In the third decision of this judicial saga, the Italian judge made a distinction between phonograms, audiovisual works and software deciding that the prohibition provided by article 6 of the Directive concerns only the first one. Once again the video game is assimilated to software, and the use of the mod chip is validated.

The Italian Supreme Court, in 2009, pronounced itself in favor of a complex qualification of the video game, which means that the protection against the circumvention of technological measures of protection applies to them.

This approach can be criticized because it focuses only on video game, where the main target of the mod chip is the console itself. By this way, the difficult question of the determination of the legal nature of video games is avoided. The operating system of the console is clearly a computer program. Does a mod chip or homebrew software, which interferes with the normal execution of the computer program, infringe the copyright of Sony upon it?

Another approach, which has the author's preference, would have been not to refer to article 6 of the Infosoc Directive, but to the older Directive of 1991 about computer programs, which has been recently codified (The directive 2009/24/EC on legal protection of computer programs). Article 6 (1) establishes an exception to the rights of the creator of a computer program where this is necessary to achieve interoperability. Under the light of this exception, the answer to the question of mod chips and homebrew software is deemed to be contrasted according to the real purpose of the modification. While a modification which adds some functionality to the console should be seen as part of the rights of the lawful user, the modification which is used for goals other than to achieve the interoperability of an independently created computer program, at the opposite, will fall under the scope of application of article 7 (1) (c) of the Directive (prohibition of circumvention of Software protection: (c) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program.

## 2. Video games and law of contracts

The legal framework of the video game industry is characterized by a triangular relationship between the consumers of the products, -the players-, the company which publishes the game and the creators. As the nature of the video game changes gradually, this relationship strengthens itself with new obligations for every side of the triangle.

### 2.1. End User License Agreement (EULA)

Almost all the video game licenses possess an End User License agreement (EULA). It is an evidence to say that this license is imposed to the player. When the consumer buys the DVD of the game, the license appears in a window with the mention "accept or refuse", but there is no real choice: the player has already bought the game and the seller won't take it back since it has been opened, and, of course, the game won't be installed if the player does not choose the "accept" option. Also, these licenses most of the time stipulate that the buyer of the game is bound by all future modification of the EULA, provision which is certainly by itself an example of an unfair term<sup>8</sup>. The EULA regulates the conditions of use, the updates and guaranties of the video game, but also, and this is a domain which becomes more and more important every day, the conditions of access to the online services offered with the game.

In Europe, a first legal approach would be to apply the Directive on abusive terms between a professional and a consumer, since it is undeniable that the EULA is not negotiated individually. Then, each term of the EULA which demonstrates obviously an inequality in the relationship will be deemed as non-existent.

An American decision went even further. In the decision of the United States District Court for the Eastern District of Pennsylvania, in 2007, a judge had to pronounce on the EULA of the famous game "Second life". Second Life creates a virtual reality where it is virtually possible to do apparently anything. A player conceived a way to buy lands (virtual lands) at a lower cost than the official market. He connected to auctions that were not public yet and bought lands for 300 dollars, while their public price was 1000 dollars. The society which runs the game decided to close his account because of the violation of the EULA and the player claimed that due to this he has lost all his virtual properties of an estimated value of 4000 dollars. The judge qualified the contract as a contract of adhesion and limited this holding by noting that a claim that a contract is one of adhesion can be defeated if there are "reasonably available market alternatives" available to the weaker party. Here it was not the case, since "Second Life" is

---

8. French TGI Nanterre, UFC Que Choisir / AOL France 2<sup>nd</sup> of June 2004.

a unique service which proposes in a massive multiplayer environment to buy some kind of virtual real property. In conclusion, the Court decided not to apply the terms of the contract.

Most EULA include various terms which could be described as unfair, such as classic terms about exoneration of liability, but also terms specific to video games, such as the restriction of copyright of the players. Indeed, the video games nowadays encourage the players to create their own personages, stories, even sometimes their own universes. The editors bet that they will create this way a community of fans who will add a plus-value to the game. It is quite a new domain of the law of copyright, the distinction between actions of the players, which are just a mere execution of the predetermined script of the video game and original intellectual creations, which should receive a protection by copyright law. One thing is sure that the EULA can't decide that all creations in all circumstances derived from the original video games are the property of the editors of the video game. This is characteristic of an unfair term and, also, violates the principle of specialty of the transfer of right which applies in many copyright law systems, a principle which requires that every transfer of copyright must be specifically defined and limited.

At the end, it depends of the particular qualities of each game. In a game like "World of Warcraft", the possibilities of original creations of the player are more limited and the term which gives all copyright prerogatives to the company does not seem unfair. However, the violation of the EULA does not mean that a work of mind is infringed automatically. In a recent decision in USA, *MDY Industries, LLC v. Blizzard Entertainment et al.*<sup>9</sup>, the judge had to decide on the case of a computer program which permits to the player to play automatically ("like a bot" to use the gamer vocabulary) in order to level-up faster. The court explained that, although the use of "bots" was prohibited by the WoW Terms of Use, it did not follow that operating outside of the scope of the license resulted in copyright infringement. For this to happen, the licensee's action must (1) exceed the license's scope, and (2) implicate one of the licensor's exclusive statutory rights<sup>10</sup>. In this case, the anti-bot provisions of the Terms of Use did not implicate copyright law. So, although "a Glider user violates the covenants with Blizzard," it "does not thereby commit copyright infringement because Glider does not infringe any of Blizzard's exclusive rights [such as alter or copy World of Warcraft software]." The Court stated that: "*Were we to hold otherwise, Blizzard — or any software copy-*

---

9. *MDY Industries, LLC v. Blizzard Entertainment et al.*, No. 09-15932 (9th Cir. December 14, 2010).

10. Joshua S. Jarvis, *Blizzard Owns Your Software*, 10.-1.2011. <<http://www.trademarkandcopyrightlawblog.com/2011/01/articles/copyright/update-blizzard-owns-your-software>>.

*right holder — could designate any disfavored conduct during software use as copyright infringement, by purporting to condition the license on the player's abstention from the disfavored conduct. The rationale would be that because the conduct occurs while the player's computer is copying the software code into RAM in order for it to run, the violation is copyright infringement. This would allow software copyright owners far greater rights than Congress has generally conferred on copyright owners.*"<sup>11</sup>.

Two contractual relationships appeared with the emergence of the massive multiplayer video game, the transfer of a virtual asset and the transfer of a virtual service. The first kind of contract refers to some virtual equipment or character, which is rare and, therefore, valuable. Is it possible to sell it? Or to steal it? It has been advanced that the philosophical theory of Locke on the justification and emergence of the right of property should apply<sup>12</sup>. The second kind of contract, the transfer of virtual services at first sounds strange. It is incredible for the non gamer to discover that a whole new economy has emerged, as described in the recent documentary<sup>13</sup> "Goldfarmer". Goldfarmer is the name given by the player to persons, Chinese most of the time, who work on a video game 8 hours a day just to level-up characters that they can sell to young and impatient American clients.

The EULA rule in the most cases (with the notable exception of the game "Second Life") the both aspects: the player is not entitled to any rights on his virtual assets and every commercial use of the game is prohibited. But if we accept that the legal effects of the EULA are limited, the following question pops up. How to qualify these contracts? More and more States are concerned about the non-taxation of virtual assets. Within the same scope, the mechanisms of unjust enrichment in Europe could be used in cases where the account of a player has been deleted by mistake. The editor could be obliged in this case to compensate for the virtual assets lost due to this operation. Besides, the companies are starting to change their position about the commerce of virtual property. Thus, Sony online Entertainment organizes itself the auction for virtual objects of its world "everquest II" with a 10% remuneration.

But at the end, virtual property cannot be recognized as true property in the legal sense. What would happen if the video game company decides to close its serv-

---

11. *MDY Industries, LLC v. Blizzard Entertainment et al.*, No. 09-15932 (9th Cir. December 14, 2010).

12. F. Gregory Lastowka & Dan Hunter, *The Laws of the Virtual Worlds*, 92 Cal. L. Rev. 1, 44-50 (2004).

13. <<http://chinesegoldfarmers.com>>.

ers<sup>14</sup> or just to introduce a new weapon or a new rule which renders the virtual property of the gamer useless? *"In Taiwan, virtual property is considered movable property and stealing such property can result in imprisonment"*<sup>15</sup>. At first, and more particularly if it is not forbidden by the EULA, we should accept that these contracts are enforceable<sup>16</sup>. In my opinion, two distinct questions have to be asked: what is the legal qualification of these virtual goods and who is the owner.

Under an economic approach of law, every act which produces some value leads to a creation of a form of property. The virtual goods create a real property<sup>17</sup>, but if the player has the *usus* and the *fructus*, it is impossible to recognize to the player the *abusus* in the continental legal tradition. Or to take a common law approach, we should consider that the player is somehow a trustee of the virtual goods. He has some rights according to the condition of the trust to sell and make profit of his virtual assets, but the beneficiary of the trust, the company, has the option to take back the ownership of the good. The problematic could be resolved also by reference to the concept of derivative works, given that the virtual assets possess enough originality.

## ***2.2. The Video Game as a provision of services***

Since the contractual relationships concerning videogames are nowadays more a provision of services than a contract of sale, the legal rights of the player have evolved, but, concurrently, the obligations of the editor have changed. The most illustrative example of this change is given by the very recent actuality. The Sony network for online video game for PlayStation users has been hacked and millions of confidential information, such as the credit card number of the players, has been stolen. Could this constitute a breach of an implicit term of the contract?

In USA, a class action has been opened against Sony, for its failure to protect the personal data of its consumers. In Europe, the situation is more complicated: class action does not exist and each player should sue individually Sony. Moreover, in most European countries, the judge in civil actions does not grant anymore punitive damages. The player would have to prove the actual prejudice of the failure of Sony. In Canada, some lawyers have advanced a radical argument: the fall of the network of one of the protagonist worldwide in the domain of new technologies is somehow synonym of despair and fear. If Sony can't protect our

---

14. Bennett, C. Massively multiplayer games and the law. In Internet and e-commerce law in Canada. (2007.08) 8 I.E.C.L.C. p36.

15. Spratley D., Virtual property and the law, available at [www.davis.ca](http://www.davis.ca).

16. Bennett C., Contracts in the MMO world. [www.VideoGameLawBlog.com](http://www.VideoGameLawBlog.com).

17. DahCunha N., Virtual property, real concerns, Akron Int. P.J. 4 n.1, 2010 pp. 35-72.

personal data, who can you trust? How many times a day should anyone consult his bank account and how much he can trust the bank anymore? By consequence, their client asks for one billion dollars of damages.

Another issue of this phenomenon is related to the information given to the victims. In these situations, victims are not only the companies that suffer the hacking, but also the users as victims of personal data leak. The video game companies could be, thus, tempted to avoid any liability just by hiding the fact of the hacking. Thus, the players would be victims without knowing it. This issue has been envisaged by the recent Directive<sup>18</sup> 2009/140 on electronic communications networks and services, which obliges the companies to declare every breach of personal data that they are aware of.

### ***2.3. The legal relationship between the creator and the editor***

A new trend appears also with the development of a new market for the video game: the smartphone. The video games for smartphones are simpler, smaller and cheaper. With the democratization of almost knowledge, everyone could decide to create his own video game. We assist in the domain of the video game a kind of return to the origins, where creators and editors were dissociated. However, the contractual relationship between the creator and the editor of the game cannot be described as equal.

Once again, the practices of the protagonists of the industry of new technologies deviate a lot from legal orthodoxy. For example, the very recent decision of Amazon to offer video games with discount created a lot of reactions. The contract that Amazon proposes stipulates that Amazon has every right to freely modify the price of the games. It is a classic term in these contracts, in order to give a legal framework to the special sales and reductions that are organized from time to time. In all cases, the creator of the game receives as royalties 70% of the retail price. But another term of the contract provides that the creator of the game is entitled to receive only 20% of the original price if these 20% are superior to the 70% of the retail price. This leads to important differences as regards the remuneration of the creator. Let's imagine a successful video game, in order to gain some clients from its competitors, could decide discretionarily to offer a discount on the game and the creator of the game will be bound by the contract to accept a decrease of his royalties.

---

18. Directive 2009/140 amending Directives 2002/21, 2002/19, and 2002/20 on electronic communications networks and service. Official Journal of the European Union L 337/37, 18.12.2009.

### **3. Conclusion**

The purpose of this paper was, throughout this short tour to the law of video games, to highlight the main debates arisen recently in this constantly evolving domain. From the classic issue of the legal definition of video games in the frame of copyright law, we reached a new challenge, this of the qualification and of the legal effects of the transactions of virtual assets. The virtual worlds are a new whole world of gaming for the players, of course, but also a new whole world which is offered for discussion for the IT lawyers. But it could be an error to believe that these discussions are only rhetorical. With 50% of the population of developed countries playing video games and with the everyday development of new smartphones applications, what is at stake about virtual reality becomes very real.

# Copyright holders and peer-to-peer network users: an uncompromised relationship?

---

---

Archontoula Kapsi

---

---

The technological evolution of the last years enabled the transmission of cultural works in a series of bits. Internet has created new practices such as file-sharing through peer-to-peer networks which are nonetheless harmful for Intellectual Property Rights. Intellectual Property content is digitized, compressed, downloaded, copied and distributed through the Internet all over the world. The tendency to share files in a digital form is massive enough to make it a social phenomenon. Indeed, in France, nearly half of all Internet users (49%) seem to use cultural content illegally, according to a study conducted by the «Haute Autorité pour la Diffusion des (Oeuvres et la Protection des Droits sur Internet» (roughly translated as the “High Authority for the Distribution of Creative Works and the Protection of Rights on the Internet”), on 23<sup>rd</sup> of January 2011, in Cannes. According to this report, illegal practices decrease according to age: from 15 to 24 years old 70% reported using cultural content online illegally as compared towards a rate of 55% when it comes to the 25-39 years old group and 32% as for those over 40 years old. The spread of internet usage for file sharing is a direct challenge to the very foundations of intellectual property rights; this challenge calls for the formulation of new policies which will take into account the practice of file sharing between internet users and the obligation to protect intellectual property.

In this context, it would be interesting to examine the arguments and conflicting interests of peer-to-peer users “vis-à-vis” those of the copyright holders in order to better understand the subject/issue. More specifically, we will analyze the various forms of use of peer-to-peer networks and the reasons leading network users to downloading. In parallel, a short recall of creators’ fundamental Property Rights (moral and patrimonial), as applied in the digital environment, will highlight the conflicting basis of this relationship. On this basis, we will then try to analyze the consequences of this interaction. It is merely about a legislative attempt to strike a balance between the different interests through the implementation of measures that limit them, and through the introduction of strict legal measures which may nevertheless undermine Internet users’ privacy, thanks to the strong willingness of governments to tackle this issue. Within this framework, it is also examined how the participation in file-sharing via network activities - as a method of distributing cultural content - is handled by courts in many parts of the world in regard to intellectual property law.



## I. The conflicting interests

### *a. The technical architecture and the key to the success of peer-to-peer networks*

Peer-to-peer is a technology that enables the exchange of digital files (audio, video, etc.) among different users, simultaneously connected to the internet. The internet users can act either as the 'server' or as the 'client' in the exchange process. Users upload files that then become available for downloading by other users of the peer-to-peer networks. This can be a recurrent procedure. There are two types of architecture in peer-to-peer networks: the centralized and the decentralized models. The centralized type of architecture is composed of a central server, to which all users are connected directly. It centralizes all the files provided by network users, allowing all Internet users to conduct a research of files (videos, photos, software, etc.) through a central database. *Napster* is perhaps the best known peer-to-peer network of this type. This software had created a file-sharing network requiring a search engine and a central server in which were listed all the available files. The exchange concerned mainly Mp3 files. This was the first network to allow connection among several millions of users, representing the most well-defined example of 'peer-to-peer centralized networks'.

However, it was on July 1999, when the Recording Industry Association of America (RIAA) was turned against the company *Napster* on the grounds that the company intentionally facilitated the illegal sharing of music files. After a two-year litigation in the United States for violating the American law on copyright, the company *Napster* ceased file-sharing activities in September 2002. The judicial difficulties faced by *Napster* that led it to cease its operations as a peer-to-peer network, the reason why new file-sharing networks have been developed based on the absence of a central server and/or a central database and focusing mainly on the use of 'peer nodes'. This 'decentralized' network model establishes a connection with one or more peers (i.e users) using the same software. All connections are based on the same principle: to launch the search, users should be connected to one or more search machines/users, which in their turn, are doing the same thing, and so on. *Gnutella* is the spearhead of decentralized networks. After the closing of *Napster*, peer-to-peer users turned to this new protocol which is a further step for the architecture of peer-to-peer networks. *Kazaa*, *Grokster*, *eDonkey* and *Morpheus* are other well-known examples of this type of decentralized peer-to-peer networks. However, in recent years, new peer-to-peer networks have been developed, based on the combination of centralized and decentralized systems, using multiple computers as servers with increased internet access power ('super-nodes'). According to this new type of peer-to-peer technologies, the role of users varies depending on each computer and on the internet connection

speed. The request of a file of each user is directed to a computer (i.e user's machine) that serves as the super-node. This super-node, actually, holds its own database but it can also search the file requested through other machines (i.e computers). Once the file requested is found, the user who submitted the request can download it directly from the user's computer that provides it. *Bittorrent* has been, in recent years, the most used peer-to-peer network of this type that facilitates broadband distribution. By optimizing the maximum bandwidth of file-sending and receiving, this new application is preferred by the public.

This free and direct exchange of digital files between users through peer-to-peer networks gives room for discussion about this new technology. With a deeper view to the matter we can clearly see that the services of these networks are not limited to the simple exchange of files.

First of all, the peer-to-peer network technology can be used in the field of education in order to enable teachers to receive and send various educational resources such as courses, works or even training methods. Training and teaching processes are therefore enhanced by this exchanging practice while the principle of collectiveness is strengthened. Moreover, the use of peer-to-peer networks can foster cooperation and collaboration through the exchange of documents (texts, databases, memos, etc.) between the employees of a company. 'Collaborative' peer-to-peer applications can also include instant messaging, chats and online games (such as *NetMeeting*, *Groove* etc). Among the various services offered by these free networks, we could also include the 'distributed computing' peer-to-peer services which allow peers to bring their computing power together in order to solve a computationally intensive problem. In the case of malfunction of centralized networks, the peer-to-peer technology can guarantee data-processing security but also encourages the dissemination of protected works or even the normal operation of phone services (e.g *Skype*). Peer-to-peer 'storage' services can also provide virtual stable storage allowing peers to continuously access files while preserving author anonymity (*Freenet* is an example of such systems). Finally, peer-to-peer multimedia streaming services (e.g *Freecast*) let peers stream and broadcast audio and video among each other.

Nevertheless, downloading of cultural content is still the most widespread peer-to-peer service. However, we can observe different kinds of use of peer to peer networks for downloading, depending each time on the special needs of internet users. Indeed, for some users downloading simply facilitates their purchases in the real market in the sense that they can obtain information on the quality and price of a product online before buying it in a real shop. On the other hand, works available in traditional forms (CDs, DVDs, etc.) still attract consumers' interest given that the quality of downloaded files through peer-to-peer networks is

not always good enough to satisfy them. For this category of users, downloading of files is merely seen as a secondary option than fundamental. However, we can observe another kind of users who do not contribute to the networks even though they benefit from them. This non-cooperative behaviour, almost passive, has two types: the “free riding” and the “easy riding”. Regarding the first type, the user does not contribute to the network since he/she has by all means access to the service and to commonly shared contents provided by other users. In this way, he/she does not bear the cost of the cooperation in such networks, such as technical (e.g. viruses or spam) or even legal risks (penalties for illegal diffusion of contents). As for the “easy riding”, it is the type according to which the user contributes to the service in order only to receive files. In this case, users share their content in order to get the files (content) they wish but once they have received this content they cease the cooperation. However, both abovementioned types can undermine the effectiveness of peer-to-peer technologies, reduce the speed of transmission and decrease peer-to-peer systems’ utility.

The phenomenon of downloading files related to cultural content through peer-to-peer networks has clearly gained much support. However, what is the key to the success of this new technology? What are the potential changes in consumption patterns of users?

We can observe a variety of reasons leading to the downloading of files through peer-to-peer networks. One of the main reasons is the cost of the original work especially for what concerns musical or cinematographic works being downloaded through peer to peer technologies. Indeed, the public is discouraged by the high market cost of music works and/or movies either in stores or through online platforms where people must pay in order to download music or films (e.g. iTunes store). Many people cannot have access to culture because they cannot afford it. In such a context, the availability of cultural works via peer-to-peer networks over the Internet plays a fundamental role in encouraging users to opt for this new technology. In fact, this new network can guarantee to everyone a free, faster and cheaper access to cultural works.

Furthermore, peer-to-peer networks undoubtedly offer a wide variety and extent of availability of contents. Users can find various music albums or film productions, new or sold out in the traditional market in total availability. Another benefit could be the existence of subtitles in many different languages for the uploaded movies, which, coupled with the transaction speed, lead the public to downloading. In addition, through these new developed networks, users have the opportunity to discover new artists and producers who are not yet promoted by the current regime of trade. Consequently, peer-to-peer networks fulfil the needs for and expectations of cultural stimulation of consumers at the lowest possible price.

Finally, the need to 'test the product' is another reason that may lead people to use peer-to-peer networks. More specifically, users have the opportunity to test and evaluate the content and then decide whether to purchase or not. The peer-to-peer technology offers a sense of security regarding the users/consumers' choice of purchase, justifying their inclination to massive downloading of copyrighted works.

However, the distribution and exploitation of Intellectual Property contents by peer-to-peer users without the prior consent of the copyright holders can threaten creators' fundamental rights, raising political and legal uncertainties. In order to better understand the issue, it is essential to analyze in advance the Intellectual Property Rights, as they are applied in the digital environment.

### ***b. The intellectual property rights applied in the digital environment***

European Union member-states generally have a common legal basis on Intellectual Property Rights (moral and patrimonial), complying with international and European Union legal instruments.

Generally speaking, the moral right of the author is divided mainly into the following basic privileges: a) the right to decide on the (first) disclosure of his/her work to the public, but also on the mode and time of publication; b) the right to respect to his/her work, that is to say, the right to oppose to any modification or alteration made on the work; c) the right to authorship, which allows the author to claim that his/her name shall be mentioned on his/her work or even the right to publish the work anonymously or pseudonymously; and finally d) the right to repentance and withdrawing, according to which the author has the right at any time, after the publication of his/her work, to prohibit exploitation by third parties or even revise of the work.

But how these rights applied in the environment of new technologies could be threatened?

With regard to the right to decide on the disclosure of the work, since the author has also the exclusive right to the first publication of his/her work, this right shall apply to any publication that takes place in both the real and digital environment. In fact, undermining the moral right of the author is a fairly widespread phenomenon in networks, consisting in free circulation and exchange of works unpublished or even unfinished over the internet, without the prior consent of the author.

As for the right to the respect of the work, the author may oppose to any eventual modification to his/her work, even when it concerns non-material modifications. As far as there is digitalization (e.g. the reproduction on a Cd-Rom) of a work, the

creator could see these rights threatened. Moreover, the conversion of recordings into an analog format or mp3 ringtones may constitute a serious distortion of the original music content, since it is an operation that modifies the original sound. Similarly, the right to the respect of the author's name may be impaired to the digital environment since the reproduction of a work, as described above, is usually realized without any reference to copyright holders. Indeed, being aware of the prohibition of this kind of reproduction and in an effort to avoid the authorship right infringement, network users usually hide files by changing the authors', violating the creator's right to authorship. Thus, the provisions of the article 7 of the European Directive of 22 May 2001 [Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society], require that European Union member-states should punish all users that modify or delete any copyright-related information in electronic form.

Finally, the implementation of the right to repentance and withdrawing into the digital environment is compromised in an irreversible way because, due to the new technologies, it seems to be even easier to proceed to alteration of cultural contents which have been already published, even if the copyright holder has previously denied or prohibited such activities or intends to revise and adjust his/her work in the future, at his/her own discretion.

In addition, copyright holders have also the principal right to the exploitation of their work, distinguished into the right of reproduction and the right of representation of the work, that is to say, the author may authorize or deny any reproduction and/or representation of his/her work, made without his/her prior consent.

Indicatively, the right of reproduction means that the author has the exclusive right to decide for the registration, translation, adaptation, and/or alteration of his/her work. The right of representation enables the author to decide whether and when to communicate his/her work, and more specifically to distribute, present, perform, transmit or retransmit it to the public.

However, several international legal texts and declarations have extended, through provisions they include, the right of reproduction described above to the digital environment. For example, the European Directive of 22 May 2001 in its article 2, introduces the principle of the exclusive right of the author to authorize or prohibit "...direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part...". Thus, the concept of digitalization consists in recording an analog work into a digital form, requiring both an act of alteration and an act of reproduction. Therefore, the adaptation of an analog work to a digital platform or a cd-rom and its further storage in an electronic

platform highlights the risk of infringement of the creator's right of reproduction in the digital environment.

Similarly, the definition adopted by the European Directive of 22 May 2001 related to the creator's right of representation of his/her work, determines how this right can also be implemented in the digital environment. More specifically, the article 3.1 of the Directive reads "[authors can]...authorize or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them". The accessibility to a work by the public by means of new technologies undoubtedly consists in a form of 'public communication', as described above. Indeed, the author's right of representation may be applied and further endangered by the activity of 'streaming' which allows the user to access data files even before the ending of the downloading via peer-to-peer networks.

It would be therefore interesting to examine within the framework of peer-to-peer technologies how actually the above intellectual property rights interact with the application of these networks over the Internet.

Firstly, according to the provisions of the World Intellectual Property Organization (WIPO) Copyright Treaty of 1996 [WCT, adopted in Geneva on December 20, 1996], the exchange of protected works over the internet via the application of peer-to-peer networks consists of activities that are subject to the authorization of the author.

More specifically, peer-to-peer users, as we already examined, can make a work from their hard disk available to all internet users having installed the software necessary for the exchange of files via peer-to-peer networks (uploading). Indeed, according to the architecture of peer-to-peer networks, all works, once downloaded, are automatically made available to other users. Furthermore, uploading can also be made through digitalization of the work an activity that is which consists, as we have already mentioned above, in reproducing the work. In both cases, making a work available to other users through peer-to-peer networks, constitutes an infringement of the exclusive right of the creator to decide for the diffusion of his work in a digital environment as well.

Nonetheless, users reproduce through downloading a work on the hard disk of their computer. Indeed, storage in the hard disk of a computer constitutes an act of reproduction. Consequently, this activity is made up by registration in the computers' hardware part and, furthermore, by a procedure that allows the communication of the work to the public, contributing to the violation of the right of

reproduction. Moreover, this reproduction can also take place by burning files to a cd platform.

Faced with technological evolution and the rapid development of file-sharing networks which resulted in significant risks for copyright holders, governments have tried to find a way to strike a balance between the wide diffusion of cultural works and the preservation of authors' fundamental rights. This search of balance consists of legal measures delineating the different interests, but also of the promotion of legal solutions aiming to answer to the controversy raised by the application of peer-to-peer networks.

## **II. In search of balance**

### ***a. A reconciliation based on technical protection measures and the exceptions to copyright***

In an effort to balance the different interests, the WIPO Treaty of 1996 [WIPO Copyright Treaty (adopted in Geneva on December 20, 1996)], adapted the provisions of the Berne Convention for the Protection of Literary and Artistic Works of September 9, 1886, to the digital environment. Also, the European Directive of 22 May 2001 related to the harmonization of certain aspects of copyright and related rights in the information society, aimed to harmonize the national legislations of EU member-states in relation to Intellectual Property, after taking into account the impact of new information technologies, through the implementation of new measures aiming at the protection of Intellectual Property Rights.

Indeed, article 11 of the aforementioned WIPO Treaty on copyright, stipulates the obligation of member-states to take legal action against the distortion of effective technological measures that are used by the authors in respect of their rights on their works. In this content, article 6 of the European Directive of 22 May 2001, also requires member-states to take effective technological measures against any activity designed to cancel the protection of protected works. According to its provisions "technological measures" consist to "any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorized by the right holder of any copyright and right related to copyright ...". However, these technological measures shall be deemed effective as far as "the use of a protected work or other subject-matter is controlled by the right holders through application of an access control or protection process, such as encryption scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective".

For example, a type of technological protection measure is the Inter Deposit Digital Number (IDDN) system, which contains all the data of a protected work, as soon as reference on this work has been made on-line. The international IDDN number is designed to accompany the work in all its reproductions and representations, and the right holder can thus always be identified. Moreover, we can also identify the development of devices such as the Windows Media Audio (WMA) which allows the limitation of acts of reproduction since the protected work that has been downloaded on the Internet can be burned only twice to a cd, while it cannot be transferred more than ten times.

Thanks to the legal protection of works through the application of technological protection measures, the violation of authors' intellectual property rights is quasi controlled or even limited through peer-to-peer networks. The need to protect the fundamental rights of the author is fostered by these measures, while the prohibition of illegal exploitation of works by users is effected through international legal instruments.

On the other hand, the protection and security granted to the authors by technological measures is limited because of the legal regime of the exceptions to the exploitation of a work in favor of the users. Indeed, several international and/or European legal instruments introduce such exceptions in relation to the exploitation (i.e reproduction) of a protected work, through a 'three-step test'. This 'triple test' constitutes the legal framework of the exceptions applied to intellectual property rights of authors, striking a balance between the different interests of the peer-to-peer networks' users and those of the copyright holders.

More specifically, the three-step test appears in article 9 par. 2 of the Berne Convention, in the article 13 of the Trade-Related Aspects of Intellectual Property Rights Agreement (TRIPS) of the World Trade Organization (WTO) [signed in Marrakesh, Morocco on 15 April 1994] but also in the WIPO Treaty of 1996. However, the European Directive of 22 May 2001 foresees further exceptions and limitations to copyright, obliging member-states to adopt such measures in order to guarantee the normal application of these exceptions on author's work. Among these exceptions we can indentify the exception of a reproduction made for private use (i.e the regime of 'private copy') "on condition that the right holders receive fair compensation", which takes account of the application or non-application of the technological measures mentioned above. Thus, according to article 5 of the European Directive of 22 May 2001 which also determines the regime of the 'triple test', this exception of 'private copy' "shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the right holder".



Consequently, the regime of the exception for private copy, being limited as described above through the triple test and on a not-free basis may be implemented in the national legislation of member-States, at their own discretion, giving the opportunity to juridical cases to invoke the exception of 'private copy' in order to release the accused from penalties for infringement of copyright through peer to peer networks, as it is hereinafter examined.

We can observe that the conciliation of the interests of users and those of right holders is principally achieved through legislative means and especially through the introduction of legal provisions aiming to restrict the rights of both sides. However, the wide spread of piracy over the internet and the consequent increase of copyright infringement, often lead governments to adopt stringent legislative measures which can though threaten users constitutional rights.

***b. A regime of legal downloading and strict legal measures,  
a response to internet piracy?***

The French government has shown keen interest for the repression of illegal internet activities, not only through the introduction of strict legislation against peer-to-peer networks, but also through the implementation of preventive actions against internet piracy on a more concrete and more practical basis.

On July 2004, the establishment of a national committee against piracy and the signature of an 'anti-piracy charter' ('charte anti-piratage') can be considered as a decisive step in the fight against internet piracy in France. This initiative has three components: the first deals with the awareness of internet users in order to alert them on the dangers of peer to peer activities but also to inform them about the illegal character of the exchanges of protected works by these means. The second component aims at the promotion and development of legal offers of downloading of music files put forward by music industries in order to satisfy consumers' interests. The third component underlines French intention governments' to facilitate the conviction of internet users through the implementation of measures aiming at user's disconnection and termination of his/her access to internet.

This 'anti-piracy charter' has introduced stricter and more concrete measures against illegal downloading of files through peer to peer networks. Yet, we can observe that until today, all aspects of the charter were implemented by the French government.

Actually, it was on September 2007 when the French government assigned to Mr. Olivennes, the task to give an end to the phenomenon of illegal downloading, by implementing the provisions of the aforementioned charter. The "Commission Olivennes" aimed specifically to reconcile copyright with the interests of inter-

net users through the outlining of a legal framework. On 23 November 2007, Mr. Olivennes submitted to the President of the French Republic its report on a project agreement about the protection of cultural works through new technologies. More specifically, the measures proposed in this project aimed to encourage the promotion of legal distribution of works through the internet but also to fight against internet piracy and illegal downloading. The Commission Olivennes proposed to increase the attractiveness of the legal offer of contents over the internet through wider availability of works on legal on-line commercial sites. The report also suggested that the regime of legal downloading should be more competitive by reducing the price of online contents. Furthermore, it introduced the implementation of sanction mechanisms adapted to a system of 'graduated response' (*"réponse graduée"*). In addition, the report proposed an administrative authority in charge of supervising and controlling the efforts and actions to counteract illegal downloading by sending warning messages to infringers in case of complaints of right holders. In case they do not comply, they will see their internet subscription suspended or terminated.

All measures and goals described above were finally incorporated into the law known as "Hadopi Law" (*Loi Hadopi*) or "*Loi Création et Internet* (Law on Creation and the Internet)" incorporated into the French legislation on 12 June 2009, aiming to control and regulate internet access and to protect copyright. This legal instrument created an agency called "*Haute Autorité pour la Diffusion des oeuvres et la Protection des Droits sur Internet*" for the diffusion of works and the protection of copyright over the internet. It has the competence to protect works against digital infringements, encourages the development of legal distribution of contents on internet, supervises how users make use of these contents and finally ensures an effective regulation and implementation of technical protection measures. This authority is composed by a college and a commission for copyright protection. More specifically, this authority requires from the internet service provider to provide all the necessary information in order that the infringer (user) can be identified. Once the authority obtains this information, it sends a first warning e-mail to the users' e-mail address reminding the french legal provisions for the copyright violation. This e-mail specifies only the time of the claim; neither the object of the claim nor the identity of the claimant. In case repeated offense is suspected through internet technologies within six months, the offending internet access subscriber receives a second warning with similar content to the aforementioned e-mail message, accompanied this time by a certified letter. In case the offender fails to comply during the year following the reception of the certified letter, and upon accusation of repeated offenses, the internet service provider is required to suspend internet access of the offender, for a specified period from two months to one year. Furthermore, the internet access subscriber is

blacklisted and other internet service providers are prohibited from providing an internet connection to this blacklisted subscriber.

The law of 28 October 2009 ("loi Hadopi 2") supplements the law of 12 June 2009 as the latter has been partially criticized by the Constitutional Council of France. The new legal dispositions specify the power of the agents of the Commission for the protection of copyright, while establishing the framework for the offence due to negligence. Furthermore, the judges are granted the authority to decide for the suspension of the user's access to the internet. However, this suspension can only be extended up to one year if the alleged act constitutes a copyright infringement and up to one month in case of negligence.

In practice, this effort to fight against the phenomenon of digital piracy through the offer of alternative solutions to the use of peer to peer networks became understood by many music industries which have promoted and developed websites for legal downloading of music files, such as the well known [www.promusic-france.com](http://www.promusic-france.com). In addition, the platform Wippit has entered into many agreements with major recording industries (e.g BMG and EMI) for the online downloading and sale of music files. The number of songs available online has yet been significant, reaching about 200,000, whereas the content of Wippit has significantly increased. Furthermore, in 2007 new sites as YouTube, MySpace or Facebook made their appearance, as they allow the free and wide circulation of cultural content through 'streaming'. To protect copyright, these sites often proceed to an agreement with recording companies or producers in order to distribute legally their cultural contents.

This not with standing, the strict new measures introduced by the Hadopi Law for the fighting against internet piracy is often perceived unfavorably by the public. The investigation and further storage and exploitation of their personal data (i.e address, name etc.) via their IP address by the Authority, seems to threaten the fundamental rights on the protection of personal data of every individual. The continuous controversy between fundamental rights of each part (i.e author's and user's rights) caused by the use of peer to peer networks leads to the conclusion that the conciliation of interests has become a top priority. However, this controversy raised about peer to peer networks could not remain outside the juridical realm. Indeed, the courts all around the world are called to apply the legal instruments they have at their disposal, in an effort to strike a balance between the legal and the illegal aspects of peer to peer networks.

### III. The conviction issued by the courts

#### *a. The conviction of software distributors*

The judicial remedy for the exchange of protected works through peer to peer networks is closely linked to the gradual development of the architecture of this technology, which has shaped the judicial decisions and practices.

At first, copyright holders turned against the companies distributing the software used for the illegal exchange of works, given that tracing and accusing peer to peer users was still difficult. Adverse jurisdictions for the peer to peer networks in the United States are characterized rather by the condemnation of publishers and suppliers of software encouraging the exchange of files than by the condemnation of users of such networks. Indeed, the example of the condemnation of Napster that we analysed above, based on the fact that the company facilitated the illegal exchange of music files providing freely for this purpose the software, forms the basis of judicial decisions on peer to peer technologies in the USA. Similarly, the Supreme Court of the United States, on June 2005, came up to the point that the editors of Grokster and Morpheus, by providing the means (i.e software) to file-sharing via peer to peer networks, intended to allow and encourage the infringement of third parties' copyright. Actually, the Supreme Court focused on the demonstration of bad faith of the accused as they knew the illicit side of their action. The Supreme Court noted that the two editors had encouraged Napster users to opt for the use their software, whereas they did nothing to curb the illegal use of contents. The fact that this activity clearly constituted a source of income, led the Court to hold the defendants responsible.

More recently, the Federal Court of the U.S decided to shut down the well known "LimeWire" services of file-sharing, based on the fact that the recording companies (including Sony Music, Warner Music, EMI) claimed that they suffered irreparable damage from the illegal file-sharing through peer to peer networks. The most interesting point about this decision is that the court considered that software distributing companies can be guilty for copyright infringement, as soon as they offer services designed to download illegal files, even if these services may be used for legitimate files.

Such kinds of decisions have also been issued elsewhere in the world. For instance, in 2005, in Australia, some companies were indicted for producing peer-to-peer software. This is the case of the decision taken by the High Court of Australia in September 2005, ruling against the company "Sherman License Holdings Ltd" for violation of the copyright on protected works by using the software "Kazaa". Indeed, the company was held responsible for infringement of intellectual property on the basis that it took no action or measure against these illegal activities in order to prevent the infringement. Furthermore, even more recently, the

Court of First Instance of Paris [*Tribunal de Grande Instance de Paris 31ème chambre Jugement du 3 septembre 2009*] decided on the conviction and the further closing of the company named 'Mubility' for illegal reproduction and diffusion of programs and videos. More specifically the company finally closed on the grounds that there has been illegally disposed, via its website, a) a software named "radioblog 2.5" enabling the circulation of phonograms through the internet, under the form of playlists, while this software permitted at the same time the automatic referencing of these playlists on the website of the Mubility company, and b) a software named 'radioblog 3.1', allowing the illegal communication of phonograms to internet users through the act of downloading of the said software.

### ***b. The conviction of peer to peer users***

There has also been a change in the 'strategy' followed by copyright holders who have switched from identifying and taking the companies that distribute the peer to peer software to the court to suing directly the users. This change is due to the evolution of technology and the change of the architecture and the general functioning of peer to peer networks. The conviction of users seems to have a deterring character as it aims to clearly discourage the violation of intellectual property rights. Indeed, criminal judgements charging internet users with high penalties can clearly demonstrate the general willingness of recording industries and copyright holders to discourage peer to peer network users from sharing files. However, the protection of the privacy and security of communications are often brought up before the courts as a 'shield' by the users in order to contain the detection and the conviction of activities committed via peer to peer networks. From a practical point of view the way jurisprudence is interpreted and applied throughout the years in Europe and the United States, underlines the debate on the relationship between the interests of peer to peer users and those of copyright holders.

The Recording Industry Association of America (RIAA), brought for the first time to the courts of America, a case of illegal downloading of contents. Jammie Thomas was sentenced on October 2007, by the court in Duluth (Minnesota) to pay 222,000 US dollars for damages to six music industries including Virgin Records, Sony BMG and Warner Music, on the basis of illegal downloading and sharing of files and further violation of intellectual property of copyright holders. In 2005, the accused had made available on internet via the Kazaa network, about 1,702 music songs. However, out of almost 2,000 music files, RIAA accused the defendant only for the downloading of 24 songs. The defence claimed that it could not be proved that the accused had actually downloaded music files, whereas they underlined the possibility of misuse of the IP address of the accused by a hacker. The judge decided that making files available for downloading is sufficient enough to make someone guilty for copyright infringement. So, there was no need to prove that these songs had been downloaded by other users or by the accused itself.

This judicial case sets a legal basis for the condemnation of peer to peer users in America. Indeed, it is the first time that a dispute between a peer to peer user and the RIAA is brought before the court. On the other hand, the judge, not convinced by the arguments of the accused, ignored the fact that it is almost impossible to prove that a particular person uses a computer and proceeds to downloading via peer to peer networks at a specific time. The court actually concluded that the name appearing on the internet access bills can be enough to prove that this person is using its computer and is further responsible for the illegal downloading of files via peer to peer networks at any time. This highlights the strict policy of judges against the exchange of cultural contents through new technologies, as the peer to peer networks.

In Europe, the judicial basis for the conviction of peer to peer users, despite of putting forward privacy as a threshold for intellectual property rights, is well established upon the example of French courts. The Appeal Court of Paris in its decision of April 2007 [*Cour d' Appel de Paris, 13ème chambre, section B Arrêt du 27 avril 2007*] sanctioned the downloading of approximately 2.000 music files on Kazaa, rejecting the argument of the exception for private use of copies. The Court held that the existence of files compressed into a 'shared folder' named on as such the computer of the accused, proved that he/she knew that public could have access to his/her own files. The fine imposed to the accused was amounted to 5,000 Euros.

In other cases, the courts accepted the argument of copying for private use, as for the reproduction of works committed through peer to peer networks, acquitting users from a particular indictment for illegal reproduction. It was on 10 March 2005 when the Court of Appeal Montpellier [*Cour d'Appel de Montpellier 3ème chambre correctionnelle Arrêt du 10 mars 2005*] reiterated the decision of the Court of Rodez of 2004, according to which the limitation of copyright on private copying applies also to reproductions committed via peer to peer networks. Indeed, this case concerned the reproduction of audiovisual works (i.e almost 500 movie films) on disks by the accused, after having downloaded these movies by using peer to peer technologies. The user was finally acquitted for its act of distributing cultural works since there was not sufficient evidence that these contents had been accessed through peer to peer networks. Moreover, the judge, confirming the claims of the accused, ruled that, according to the provisions of the French intellectual property code, the acts of the accused were based on the exception of private copying. Similarly, the decision of the Court of Bayonne on 15 November 2005 [*Tribunal de Grande Instance de Bayonne, Jugement du 15 novembre 2005*] held that the act of downloading MP3 files via the peer to peer software 'Kazaa' was neither a crime of concealment, nor an act of illegal copying of music. Therefore, the judge ruled that '... by storing on the hard disk of his computer music content, or by burning them to CD ROM, the accused had simply exercised its right to establish a copy for personal use; so, he should be acquit-

ted of the surplus continued (...) the accused had not any purpose of personal enrichment, it was in a precarious situation, and that a basic sentence should be imposed.. “. The judge considered that it was not possible to quantify the exact number of acts of file-sharing. Finally, the user who made protected files available to other users was only sentenced to a fine of 750 euro on the basis of ‘uploading’ and to 700 euro for damages.

However, the juridical handling of these issues related to peer to peer networks by the courts of the United States and European countries, as analyzed above, may highlight the instability that characterizes the judicial crisis related to these technologies. In fact, the particularities of peer to peer technologies imply that the conviction of peer to peer users can be subject to diverse opinions with regard to its effectiveness against copyright piracy through the internet. This happens because of the existence of a legislative shield for peer to peer users, as we examined above, that ensure the legal exploitation (i.e reproduction) of works upon the condition of private use. The harmonization of different interests seems therefore to be more complicated or even unrealistic. In fact, the evolution of new practices of copyright infringement, such as the development of web services (i.e. YouTube, Dailymotion or Myspace etc.), but also new types of offences via new technologies, render the conciliation of the different interests a complex issue.

Copyright holders and peer to peer users are in an ongoing debate that is developing at a rapid and steady pace. We can observe the (very) nature of this conflict through legislation, but especially through jurisprudence, where the opposing parties put forward their arguments and claim economic or moral compensation. The need for a conciliation of interests becomes imminent. But, the attempt to seek solutions to the phenomenon of peer to peer networks under different perspectives is always made on a legal basis. Indeed, for all governmental institutions the solution to the problem is, the balance between the different parties which can be found in the application of the law. According to the legislator, the balance can be stricken by means of legislative provisions and the legal limitations applied to the opposite interests. The different interests can therefore be put forward in accordance to the interpretation of the jurisprudence by taking into consideration the special circumstances, in an effort to maintain an impartial and fair stance. My personal opinion is that this is not enough; in order for any solution to be viable it has to depend not only on the provisions of the law but also on our individual moral principles and respect of others.

*“The right to swing my fist ends where the other man’s nose begins”*

(Oliver Wendell Holmes, Jr., Jurist)

## References

### Books

Sinodinou Tatiana-Eleni (2008) Intellectual Property and new technologies: the relationship of the user and the creator, Sakkoulas, in Greek.

Barbet Philippe – Liotard Isabelle (2006), *Sociétés de l'information: enjeux économiques et juridiques*, L'Harmattan.

Delprat Laurent – Halpern Céline (2007), *Communication et Internet: pouvoirs et droits*, Vuibert.

Feral-Schuhl Christiane (2006), *Cyberdroit: le droit à l'épreuve de l'Internet*, Dalloz.

Guinchard Serge – Harichaux Michèle – Tourdonn Renaud (2001), *Internet pour le droit: connexion, recherche, droit*, Montchrestie.

Lucas André (1998), *Droit d'auteur et numérique*, Litec.

Quemener Myriam – Ferry Joël (2007), *Cybercriminalité: défi mondial et réponses*, Economica.

Ravaz Bruno – Retterer Stéphane (2006), *Droit de l'information et de la communication*, Ellipses.

Wekstein Isabelle (2002), *Droits voisins du droit d'auteur et numérique*, Litec.

Lucas André (1998), *Droit d'auteur et numérique*, Litec.

### Articles

Auroux Jean-Baptist (December 2007), *Rapport olivennes: les grandes lignes de la loi DADVSI 2?* Revue Lamy Droit de l'immatériel, n. 33.

Bauwens Michel – Remi Sussan, (2005) *Le 'peer to peer': nouvelle formation sociale, nouveau modèle civilisationnel*, Revue du Mauss semestrielle, Alter-démocratie, alter-économie, n. 26.

Coulaud D Mathieu – Mariez Jean-Sébastien, (January 2008) *L'évolution de la protection des œuvres sur les réseaux numériques ou le choix du mode contractuel*, Revue Lamy Droit de l'immatériel, n. 34, 55.

SINGH Asim, (June 2007) *La qualification juridique des actes accomplis dans un réseau 'peer to peer'*, Revue Lamy Droit de l'immatériel, n. 28.



## Internet

Munindar P. Singh, Shengru Tu (2009), *Free riding in peer to peer networks*, online at: <[http://www.cs.bilkent.edu.tr/~p2p/ieee\\_internet\\_computing.pdf](http://www.cs.bilkent.edu.tr/~p2p/ieee_internet_computing.pdf)>/accessed 18.3.2011.

Synthèse du Forum de Discussion (2003), *Peer to peer: quelle utilisation pour quels usages?* online at: <<http://www.foruminternet.org/telechargement/documents/syn-p2p-20030620.htm>>/ accessed 18.3.2011.

Text of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, online at: <[http://www.wipo.int/wipolex/en/text.jsp?file\\_id=126977](http://www.wipo.int/wipolex/en/text.jsp?file_id=126977)>/accessed 19.3.2011.

Text of WIPO Copyright Treaty (adopted in Geneva on December 20,1996), online at: <[http://www.wipo.int/export/sites/www/treaties/en/ip/wct/pdf/trtdocs\\_wo033.pdf](http://www.wipo.int/export/sites/www/treaties/en/ip/wct/pdf/trtdocs_wo033.pdf)>/accessed 19.3.2011.

Text of Uruguay round agreement: TRIPS, trade related aspects of intellectual property rights, online at: <<http://www.wipo.int/treaties/en/agreement/trips.html>>/accessed 20.3.2011.

Text of LOI n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (1), online at: <<http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&fastPos=1&fastReqId=1885736834&categorieLien=id&oldAction=rechTexte>>/accessed 19.3.2011.

Text of LOI n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet (1) online at: <http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021208046&fastPos=1&fastReqId=1775307367&categorieLien=id&oldAction=rechTexte>/accessed 20.3.2011.

Le Forum des Droits sur Internet (2005), *Peer to peer: la Cour Suprême des Etats-Unis d'Amérique condamne...un business model*, online at: <<http://www.foruminternet.org/specialistes/veille-juridique/actualites/peer-to-peer-la-cour-supreme-des-tats-unis-d-amerique-condamne-un-business-model.html>>/accessed 20.3.2011.

Sébastien Delahaye (2007), *Justice et piratage: 9250 dollars par chanson téléchargée*, online at: <<http://www.ecrans.fr/Justice-et-piratage-9250-dollars,2265.html>>/accessed 20.3.2011.

Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (2011), *Hadopi, biens culturels et usages d'internet pratiques et perceptions des in-*

*ternautes français*, online at: <<http://www.hadopi.fr/download/hadopiT0.pdf>>/accessed 21.3.2011.

International protection of author's rights and neighboring rights online at: <http://www.iddn.com/> accessed 25.3.2011.

LE MONDE (13.5.2010) *Téléchargement illégal: Limewire reconnu coupable*, online at: [http://www.lemonde.fr/technologies/article/2010/05/13/telechargement-illegal-limewire-reconnu-coupable\\_1350848\\_651865.html](http://www.lemonde.fr/technologies/article/2010/05/13/telechargement-illegal-limewire-reconnu-coupable_1350848_651865.html)/accessed 21.3.2011.

Discours et communiqués, *Charte d'engagements pour le développement de l'offre légale de musique en ligne, le respect de la propriété intellectuelle et la lutte contre la piraterie numérique*, online at: <<http://www.culture.gouv.fr/culture/actualites/conferen/donnedieu/charte280704.htm>>/accessed 22.3.2011.

Le développement et la protection des oeuvres culturelles sur les nouveaux réseaux (2007), *Rapport au Minister de la Culture et de la Communication* online at: <<http://www.culture.gouv.fr/culture/actualites/conferen/albanel/rapportolivennes231107.pdf>>/accessed 22.3.2011.

Text of the decision of *Cour d'Appel de Montpellier 3ème chambre correctionnelle Arrêt du 10 mars 2005*, online at: <[http://www.legalis.net/jurisprudence-decision.php3?id\\_article=2035](http://www.legalis.net/jurisprudence-decision.php3?id_article=2035)>/accessed 22.3.2011.

Text of the decision of *Tribunal de Grande Instance de Bayonne Jugement du 15 novembre 2005*, online at: <[http://www.legalis.net/jurisprudence-decision.php3?id\\_article=1559](http://www.legalis.net/jurisprudence-decision.php3?id_article=1559)>/accessed 22.3.2011

Text of the decision of *Cour d'Appel de Paris, 13ème chambre, section B Arrêt du 27 avril 2007*, online at: <[http://www.legalis.net/jurisprudence-decision.php3?id\\_article=1954](http://www.legalis.net/jurisprudence-decision.php3?id_article=1954)>/accessed 22.3.2011.

Text of the decision of *Tribunal de Grande Instance de Paris 31ème chambre Jugement du 3 septembre 2009*, online at: <[http://legalis.net/spip.php?page=jurisprudence-decision&id\\_article=2714](http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2714)>/accessed 22.3.2011.

# **Surveillance in the workplace: new technologies, new challenges, new solutions?**

---

**Eleni Karakolidou & Lilian Mitrou**

---

## **1. Introduction**

Technology plays a significant impact on our lives, changing the way we live and communicate and - last but not least - we work. In a steadily changing environment employees are becoming not only users of technology tools but also objects of data collection and surveillance. Traditionally, the terms of employment entail collecting a considerable amount of information about employees, as these data are necessary for basic management activities such as hiring, payroll processing, performance evaluation and organization security.

The terms “employee monitoring” or “surveillance” refer to activities intended to collect and record information about employees (UK Information Commissioner, 2003; CNIL, 2002). More concretely, these terms refer to employer-controlled observation of employees in order to ascertain employee performance, behaviour, and characteristics. Employee surveillance and the consequent conflicts are by no means a new phenomenon: frontline supervisors had and still have the duty to perform employee surveillance as a means of managing the workforce and protecting the workplace. Opening a letter or monitoring an employee’s telephone conversation raised actually the same issues. It is important however to consider that the wide availability of monitoring technology facilitates and multiplies the monitoring possibilities of the employer (Mitrou and Karyda, 2006). The main reasons for that have been attributed to the lowering costs of the technology, as well as to the increasing need companies have to protect their infrastructure, especially after 9/11. As enabling technology has been advanced and become available at a lower cost, it has become significantly easier for employers to monitor employee performance or e-mail and internet usage in the workplace (Suda, 2005).

Although the protection of privacy seems sometimes to be a concern for both organizations and employees, these have different perspectives: for employees, it is important to know that their informational and communicational privacy and dignity is respected. Employers, on the other hand, need to prevent illegal actions, or actions that could jeopardise the security of the information and communication systems. Undoubtedly, an employer has a legitimate right and inter-

est to run her business efficiently and the right to protect her property and herself from the liability or the harm that employees' actions may cause. On the other hand monitoring poses risks of intrusions on the employees' privacy, data protection and freedom of communication. These risks become particularly high in the modern information society where the boundaries between professional and private life are blurred (Iglezakis, 2009).

Do employees abandon their right to privacy every morning at the doors of their workplace? How can employers provide for the security of their information systems, without offending employees' rights? Can organizations adopt a balanced approach between these competing rights and interests while, at the same time, preserving their security? Technology has a *Janus face*. Privacy enhancing technologies (PET or PETs) may protect the employees' privacy rights and the use of the appropriate technology tools allows a symmetrical approach of conflicting rights and interests. This paper argues that organizations can address the standing controversy between an employee's right to privacy and an employer's need to safeguard organizational resources, by formulating use policies, which are based on principles of lawful monitoring and on existing, widely used security management standards.

The rest of the paper is structured as follows: the next section (2) provides an overview of employers' rights and interests which are served by employees' monitoring. In section 3 we discuss the employees' right to privacy and the current approaches on the debate on workplace monitoring and the employees' rights. In Section 4 we present the main surveillance techniques implemented in the work environment and we underline their impact on privacy rights. Then in section 5 we analyze privacy enhancing technologies that may be used in workplace with the aim to conciliate the conflicting rights and interests. Finally, the last section presents the overall conclusions of our paper.

## **2. Do employers have a –legitimate!- right to spy on employees?**

Employers underline that one of the most common reasons for employing monitoring technologies is their endeavour to protect their interests and the interests of their stakeholders. Monitoring methods are implemented for many reasons such as controlling and allocating costs, measuring and improving productivity. Other cost related reasons invoked for justifying employee monitoring include the cost and downgrade of the company's network bandwidth, when employees use the web and e-mail for private activities and reasons. Actually, a great number of employees are spending their working time, sending private e-mails, surfing on the Net and sending private e-mails or blogging, the so-called "cybers-

lacking" (Iglezakis, 2009). Consequently, employers tend to regard control of the workplace and the workforce as their prerogative, including the right to protect and control their property, and the right to manage employees' performance in terms of productivity, quality, training, and the recording of customer interactions (Findlay and McKinlay, 2003). The prevention or detection of industrial espionage by employees and third parties also belongs to the main objectives pursued through employee's surveillance.

Employers monitor the use of computer and communication systems in order to prevent or respond to unauthorized access to the employers' computer systems, including access by hackers or crackers and to protect computer networks from becoming overloaded. Employee monitoring seems to be indispensable as much as the so-called "insider threats" pose a significantly greater level of risk and also have a heavier cost for organizations (Schultz, 2002). Moreover, many employers have to respond to the need to verify breaches of confidentiality or monitor compliance with security rules and to prevent security breaches, which are caused, for example when employees, intentionally or unintentionally, download a virus or open a corrupted file.

The dissemination of illegal or offensive material by employees can cause bad reputation or even result to legal prosecution for organizations. With the rise of the "*blogosphere*", employers are interested in protecting themselves from defamation: employees' internet activities are checked for offensive or libellous content. Blogging about the employer, even with comments posted on private servers outside company time, has already led to dismissals (Ball, 2006).

Employers are also subject the obligation to prevent or detect unauthorized utilization of the employers' computer systems for criminal activities (Bloom et al., 2003). The control of compliance with employer's workplace policies related to use of its computer systems, email systems, and Internet access is a means to prevent and to investigate complaints of employee misconduct, including harassment and discrimination complaints. Employers use surveillance methods to discover theft and pilferage, to investigate suspected theft, and to identify possible culprits. Employees' monitoring technologies are also used for forensics' purposes, i.e. for collecting evidence for auditing and judicial purposes after an incident has occurred (Mitrou and Karyda, 2009).

In legal terms and according to the provisions of the Data Protection Directive legitimate monitoring and processing of employees' data includes data that are necessary (a) for compliance with a legal obligation of the employer, (b) for the performance of the work contract, (c) for the purposes of a legitimate interest pursued by the employer or (d) for the performance of a task carried out in the public interest (DPWP, 2001).

Doubts are expressed about the capability of the employer to legitimise monitoring through employees' consent. In the USA the reasonable expectation of workplace privacy is often reduced by the use of consent from employees: employers demand such consent as a "standard business procedure" (Phillips, 2005). As a result, consent to search and monitor is becoming implicitly acknowledged in the employment relationship. The concept of consent as a way to legitimize monitoring practices under EU law is not quite straightforward as under US law, particularly in the employment context, where withholding consent can have immediate negative jobs consequences.

The European Commission has expressed the opinion that "employers should avoid relying on the worker's consent as a means that legitimises by itself processing of personal data" (European Commission, 2002), while the International Labour Office (ILO) accepts, under conditions, employee's consent as legitimate basis for the collection of data (ILO, 1997). The Data Protection Working Party has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data, it is misleading if it seeks to legitimize this processing through consent (DPWP, 2001).

In our opinion, due to the nature of the employment relationship, in which there is an inherent imbalance of power and the employee is subordinate and dependent, reliance on consent should be confined only to the very few cases, where the employee has a genuine free choice and is subsequently able to withdraw the consent without detriment (Mitrou and Karyda, 2006). Some countries' national laws prohibit reliance on consent altogether. In Finland, "the employer is only allowed to process personal data directly necessary for the employee's employment relationship." No exceptions are permitted, not "even with the employee's consent." Many European Data Protection Authorities took the view that an employee's consent may not lift the general prohibition against abuse of purpose.

### **3. Privacy in the workplace?**

The issues concerning employees' privacy indicate the broader transformation that has occurred in workplace relationships over the last decades: in stable workplaces and lifetime employment relationships there was a stronger element of trust between employers and employees, which rendered surveillance and respectively privacy less significant. (Selmi, 2006). At the same time, the discussion about employees' privacy rights reflects also a fundamental re-alignment of the guiding principles of labour law: the re-direction of the emphasis upon the rights and the empowerment of the individual employee (Simitis, 1999).

Employees are routinely asked to sacrifice privacy rights to managerial interests like productivity, prevention and detection of threats and liability risks. Given

the workplace belong to the so-called “public sphere” (in contrast to the “privates sphere”), American courts and authors argue that employees, who are hired to attend company business, cannot have a “reasonable expectation of privacy”. Furthermore, they justify the lack of privacy, by referring to the fact that communications are voluntarily taking place inside the premises with the use of the equipment designated to serve business objectives (Fazekas, 2004). Moreover, in the employment context privacy, if any, seems to be exchanged for something of commensurate value, like taking or keeping a job (Lasprogata et al., 2004).

Regarding privacy as a purely bargainable and alienable right, ignores the dignity element, inherent in the notion of privacy: as related to privacy, dignity summarizes, among other principles, the recognition of an individual's personality, respect for other people, non-interference with another's life choices, possibility to act freely in society (Rodota, 2004). The American approach in this area seems diametrically opposite to the situation in Europe: Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states: “everyone has the right to respect for his private and family life, his home and his correspondence”. The more recent Charter of Fundamental Rights of the European Union affirms that “[e]veryone has the right to respect for his or her private and family life, home and communications” (Art. 7) as well as the “to the protection of personal data” (Art.8). The European Court of Human Rights rejected the distinction between private life and professional life since the workplace is especially suited for social intercourse (Klare, 1982) and “it is after all in the course of their working lives that the majority of people have a significant opportunity of developing relationships with the outside world” (*Niemitz v. Germany*). A decisive criterion is the difficulty to “distinguish clearly which of an individual's activities form part of its professional life and which not” (*Niemitz v. Germany*). Respect for private life includes, to a certain degree, the right to establish and develop relationships with other human beings. The fact that such relationships, to a great extent, take place at the workplace puts limits to employer's legitimate need for surveillance measures.

The case *Halford v. the United Kingdom* was insightful for the extension of the protection of privacy in correspondence to telecommunications. The Court decided that interception of employees' phone calls at work constituted a violation of Art. 8 of the ECHR and rejected the argument of United Kingdom that the plaintiff had no reasonable expectation of privacy in those calls, as they were made using telephones provided by the employer. In the case *P.G. and J.H. v. the United Kingdom* (2004) the Court concluded that a reasonable expectation of privacy is only one criterion to determine whether an interference with the right to privacy exists. The concept of Article 8 of the ECHR recognizes the mere existence of privacy expectations in a free and democratic society. In *Copland v. the United*

*Kingdom*, the ECHR stated that the reasonable expectation as to the privacy of communications “should apply in relation to the applicant’s e-mail and internet usage”. The Court recalled explicitly that the use of information relating to the date and length of telephone conversations and in particular the numbers dialed, as “integral element of the communications made by telephone” (*Malone v. the United Kingdom*), can give rise to an issue under Article 8 of the Convention.

On the other side, the European Court of First Instance in case *Tzoanos v. Commission* took a minimalist approach to the right of privacy of public employees. The European Court of First Instance found that the European Commission could examine the computer used by Tzoanos without his presence and use the information to commence a disciplinary action against him. To justify its conclusion, the Court first pointed out that the European Commission had always been the computer’s owner and had allowed Tzoanos to use the computer exclusively for European Commission work. The court then justified its conclusion through reliance on the duty of European Commission employees to serve the interests of the European Commission.

An employer’s ability to monitor must also be balanced with considerations of employees’ morale and job satisfaction. The panoptic effect of being constantly monitored, achieved through surveillance, has negative impacts on the employer-employee relationship, which principally should be based on mutual trust and confidence (UK Information Commissioner, 2003; Desprochers and Roussos, 2001). The impacts of monitoring on employees and workplace routine is none but negligible. Monitoring not only affects employees’ privacy rights but moreover, it provokes stress and discomfort and lowers the self-esteem of employees (Mitrou and Karyda, 2006). Studies have shown that communication’s monitoring causes higher rates of depression, anxiety and fatigue (Fazekas, 2004). Last but not least, there is no research that monitoring of the employee improves the productivity (Iglezakis, 2009).

Furthermore, the surveillance of the employees communication and web surfing can lead to incorrectly results. This issue arises because the automated surveillance capture everything and the results can easily confuse and disorientate. In more detail, a virus can infect the pc and make the web requests automated without the employee’s involvement.

#### **4. Surveillance technologies in the workplace**

However, employers are looking for new surveillance measures more excessively and drastically. The new technology covers this need with new means, which can be categorized as privacy invading technologies. Widely employed surveillance technologies include communications monitoring, video surveillance, desk-



top monitoring, location monitoring and the use of biometrics. Communications monitoring entails surveillance of e-mails, web sites visited, phone calls as well as intranet and Internet traffic. The technology used to support this type of monitoring includes software monitoring and the use of firewalls, intrusion detection systems that monitor all network traffic, sniffers, passive listeners to intercept Internet communications and antivirus programs. The percentage of employers in the US using video monitoring to detect theft, violence, sabotage and other employee misconduct was raised from 33 % in 2001 to 51 % in 2005 (American Management Association, 2005).

Remote control programs which are installed on employees' computers allow control of a remote host for surveillance purposes, redirecting the video display of the remote host to another host. In this way an employer can view in real time a copy of what the employee is viewing. Desktop monitoring also includes files content monitoring. In many companies employees are equipped with *smart* ID cards which can track their location while they move through the workplace. New employee ID cards and RFID cards can even determine the direction the worker is moving at any given time. Global positioning technology (GPS systems) is also used to monitor employee cell phones, to keep track of company vehicles, and to monitor employee ID cards. The latter are also widely used for controlling physical security and access to buildings and data centers. However, Finally, fingerprint scans, facial recognition technology and iris scans are also used by a few companies for employee monitoring.

The workplace is an extremely interesting environment as far as it concerns the topology and the connection of the Information system. In particular, in a typical workplace the hosts are attached to the same LAN (Local Area Network). Consequently any information can be easily tracked and evaluated by the employer. LANs are commonly Ethernet networks that contain devices such as PCs, printers and servers over a small geographical area. Furthermore, there are many technologies, such as packet sniffer that can identify the specific IP address each employee uses via the workplace network and the content of the search or even the communication. A profane and common example is the use of proxy servers, which are intermediate systems that are configured to collect all the internet requests from the workplace hosts and then process them to the internet. The most important resource of private information is the log files, since are stored valuable private data such as the IP address and the message. Hence, the first action is to identify the IP address to the personal computer and later to the employee. As a result, there are no bounds in the information recorded (Boncella, 2001).

Another privacy-invading technology is the packet sniffer, which serves as an eavesdropper of the network. Its main operation is to ensure the security of the

network by monitoring the traffic and the security incidents. In this context it is a valuable tool in order to balance the traffic and solve connectivity or congestion issues. On the other side there is no hidden information for a packet sniffer, since it collects every data streams flow across the network (Qadeer M.A. et al., 2010). Keyloggers are also undoubtedly privacy-pervasive tools. As a matter of fact, the keylogger captures every typed character. Consequently, every keystroke is tracked revealing the content of a message or a text (Sagiroglu C. and C. Gurol C., 2009).

Moreover the capture of the packet of instant messaging and mail communication may have far-reaching impacts on employees' communicational privacy. There is a variety of ways that surveillance can be processed. First of all, if there is a server (e-mail or instant messaging) that belongs to the same company it is obvious that every transmission can be completely accessible to employers (Qadeer et al. 2010). In addition, there are many technologies that capture the packet that contains all the data, such as the packet sniffer and the keylogger. Another privacy-pervasive software is the Virtual network computing (VNC), which is a remote display system that allows any administrator to view personal computer's desktop display by remote use. The sequence of events is the transmission of the keyboard and mouse events which causes the relay of the screen (Pering et al. 2009).

Actually, with the advent of graphical desktop sharing system a Greek company breached employees' data and procedure by remote control. Considering the case of e-mail and internet monitoring the Hellenic Data Protection Authority took important decisions for the privacy issue. In particular, the case encompasses a VNC operation which provides unlimited access in the employees' personal computers and communications. As a result, the company's Information Technology and Communications department and anyone who had the relevant password could have access in the employees' personal computer and communication by distance. Moreover, the company prohibited any password alteration, even in employees' that they knew for the software existence. The Authority after taking into account the employer and employees' arguments decided that the relevant actions constituted a violation of the data protection rules. According to the Decision, the monitoring of the web surfing is an unacceptable measure, since there are and other ways of security, such as restricting the access in specific web sites. The Authority ruled that the employer had to a) inform the employees about the abilities of the software and its use, b) to allow employees to have the ability to specify their private folders and protect it with passwords, which will be inaccessible to third parties. In order to comply with law the employer should also abstain from collecting and processing personal data of employees' communication, apart from cases of monitoring cost and necessity for management the performance and troubleshooting of a specific process. The Authority regarded the recording of the content and the IP number of the communication

as strictly prohibited under the law (Hellenic Data Protection Authority, Decision of 21.4.2004).

It is obvious that all these technologies, which stem from the security field, certainly breach the employees' privacy. Indeed, the employer should take into account the legitimate rights of their employees. However, it is advisable from the practical point of view to ensure the safety of the business. The solution could be to law down both sides for an arrangement. Although, the solution should not be derogate from preserving of the employees' dignity.

## **5. Protecting employees' privacy through technology**

However, the same technologies that threaten employees' privacy can also be used to help protecting it. Technological solutions that can offer privacy protection are defined as Privacy-Enhancing Technologies (PET or PETs). The common properties of the various definitions of PETs is that these technologies reduce the risk of privacy breaching, minimize the personal data being stored, and allow individuals to keep and obtain control on their data. The European Commission in its Communication to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) states the PET as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system" (European Commission, 2002).

Generally, the PETs include a variety of technologies and processes that has as an aim to protect the content of the communication or the web request and also the anonymity of the relevant parts. In this point we must differentiate the security technologies from privacy technologies, since there are systems with both similar properties and completely different. It is advisable for a practical point of view to compare the technology as an entity and not as a type (privacy or security). In particular, there are security technologies with the privacy's properties such as encryption tools, access security tools, role based authorization that operates as privacy invasion technologies (proxy servers). Most of these techniques depend upon encryption. PETs aim to protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, while preserving, at the same time, the functionality of the information and communication system. PETs are considered to be important privacy protection instruments and are even regarded as substitute for other instruments of privacy protection, such as laws and regulatory or administrative authorities. However, PETs should be considered complementary to the regulatory privacy protection

instrumentarium, with which they must be combined in order to address the issue of privacy protection in an effective and holistic way.

To ensure the privacy of employees, it is necessary that PETS comply the main information privacy requirements: a) authorization and authentication/identification of the employee who is authorized to have access to a system, b) anonymity or pseudonymity, c) unlinkability, d) unobservability (London Economics, 2010). In view of all this facts we will categorize them in workplace privacy properties and home-network privacy properties. In particular, the Authentication, Authorization and Identification have the same main point of identification and privileges which are not suitable for the workplace. In the workplace there is a local network topology, which is under the administrator's control. Therefore, any identification uncovers the identity of the employee and cause inevitably a privacy breach. On the other hand, the rest privacy properties are suitable for the workplace and coincide with the topology's needs. Hence, the accomplishment of anonymity, pseudonymity, unlinkability and unobservability is the desirable result. However, the structure of the company creates an obstacle of anonymity, pseudonymity, unlinkability and unobservability of the one part of the communication, as far as the routing table needs the specific IP address in order to provide the path from the personal computer to the internet and the opposite. In the following section we will analyze certain privacy requirements and how they can be applied in the context of privacy enhancing technologies at the workplace. The obstacle identified at the workplace is the feature of the local network that is under the command of the administrator. In considering this issue, we rule out many privacy enhancing technologies that are not compatible with this specific environment.

### ***TTP Flocks***

The use of proxy servers, as already mentioned, may infringe the privacy rights of the employees, as the employer (usually through the administrator) can have access to the web requests and the web pages that are browsed by an employee. However, with specific configurations proxy servers can be transformed in privacy enhancing technologies. As a matter of fact, proxy server is one of the low budget solutions of privacy issues under the crucial condition that the first proxy server should be trusted! The solution of having means which do not retain or observe any personal data is unlikely due to the nature of the topology.

In contrast to common proxy servers, the TTP (Trusted Third Parties) Flocks includes the advantages that derived from the traditional properties of proxy servers and also the capability of the data and partially the connection anonymity. The data anonymity is succeeded only in the case that none of the proxy servers can determine the data of the communication. On the other hand, the partially

connection anonymity can be accomplished if no one of the proxy servers can identify the two parts of the communication. However, it is pointed out that in the company's facilities it should be considered that there is an issue of trust in the relationship of employee with the employer. Therefore, connection anonymity cannot include both the two parts, but only one of them. Furthermore, the data anonymity protects the content of the employees' data with the adequate encryption of the data. Hence, the data anonymity is accomplished by the encryption and the Trusted Third Parties. To be more specific, the TTP Flocks using independent Trusted Third Parties to transport the responsibility of privacy to them, since TTP have less interests of the monitoring.

In conclusion, the TTP Flocks reduces bandwidth and increase response times, but keeping the content and the real address hide provokes security issues. Furthermore, the issue of reliability of the first proxy server is important because it has the information of the sender and can reveal it. Hence, employer can not interfere in the data base of the Trusted Third Parties and the employees' privacy is more reliable (Liu and Olivier, 2008). In this situation we try to provide employee anonymity from employer, so if we recall that the proxy server is the employers' facility we understand that this is unrealistic. Taking all this into account, we suggest TTP Flocks as a solution for content encryption and partially connection anonymity.

### ***Squid***

Squid is a proxy, which offers an enhanced authorization, privilege control, and logging in an interface in order to manage and configure the proxy easily. The process stems from the operation of caching and reusing frequently-requested web sites. As a result an employer applying the Squid has the necessary properties of easily managed and secure software. In addition, the Squid encompasses and the common features of a proxy server. In specific, it allocates two methods of content control: one is the blocking of words in the level of software and the other is negative and positive lists. Another way of security protection of the information and communication systems is the prohibition of downloading files with concrete extensions or the prohibition of downloading files bigger than a size that is determined by the administrator of the system.

On the other hand, the Squids provides specific privacy configurations such as minimization of access in the personals data and the privileges and also minimization of time and information storage. Squids' log file contains useful information of the internet operation such as faults of system configuration, consumption of resources and information of access. The crucial file that it should be managed with caution is the access.log, which contains information of employees' activities. Indeed, the management of this file should include as less personal data as

is possible. Moreover, it must be applied further restrictions for the enforcement of the privacy such as access with code and limited privileges in the log files. Additionally, the administrator with the use of Squid can apply techniques that will ensure the employees' anonymity. An important data anonymity feature is the binding of the employees' ip address field. This action is valuable for both sides as comply with the privacy and security needs. An important anonymization feature includes the binding of the employees' IP address field which is not shown, while the administrator can monitor the selected webpages without knowing whom they have been selected by. In this way, the administrator will be able to update the address filtering, in order to maintain the security. The randomization technique is applied with the help of a filter that map the real IP addresses with false ones and the bit concealment technique is applied by encrypting the last 8 bits of the access.log file (Wessels, 2004). The only shortcoming of the privacy enhancing procedure is the lack of stability in the configurations. It is a fact from a practical point of view that the administrator can control and configure the Squid, so every alteration in the privacy configurations can cause privacy leakage, without being perceptible.

### ***Pretty Good Privacy and Off the Record Messaging***

The confidentiality of conversations of private nature is undoubtedly of major importance for the privacy of the employees. Principally, in order for their electronic communications to remain private, both the identity of the communication partners and the context of their communication should not be revealed.

PGP (Pretty Good Privacy), designed at 1991, aimed at securing the content of the message. Since then, the PGP is used also for the encryption and the signature of e-mail. In specific, PGP can be used as privacy enhancing technology, since it protects the content of a communication. A major advantage of PGP is its general acknowledgement by encryption specialists and its endurance in time. It is very important for an encryption algorithm to be used for years since it amplifies its endurance in threats and attacks. This fact, however, does not render it absolutely safe because attacks improve as long as technology develops (Nada and Al-Slami, May 2008).

The instant messaging protocol Off - the - Record Messaging (OTR), was designed at 2004. OTR provides a secure communication, since it uses encryption in order to protect content of messages and the authentication in order to ensure that a person communicates without the presence of an eavesdropper. In the context of workplace, the OTR can be used as add-on in various instant messaging software offering automated authentication and encryption. Especially, OTR protects the content of communication, with the use of cryptographic algorithm deterring any

revelation of information in the employer. Moreover, the confirmation of the two parts of the conversation is also provided (Stedman et al., 2008).

### ***Anti-keylogger***

Keyloggers detection are important for the protection of both employees' privacy and the company's critical information. The technical solutions offered for the detection of keyloggers are separated in three categories: a) software and appliances that detect and erase the keyloggers, b) software and appliances that prevent keyloggers and an c) automated program of data typing obfuscation. The third alternative allows the detection of all the keyloggers types. More specifically, the method of automatic obfuscator generates random strings, whenever the interceptor captures a keyboard event. In this case, even though a keylogger will successfully log every character that employees have typed, the employer cannot retrieve any private information from this log. The reason is the injected random length strings. With this way, the employer analyzing the log file cannot locate useful information if the process of obfuscation has a pseudorandom affect. However, this solution cannot apply against hardware-based keyloggers, because keyloggers capture the keyboard typing before it arrives at the motherboard (Chieh-Ning Lien and Chien-Chia Chen, 2008).

### ***ISO 27002***

The ISO/IEC 27002:2005 can improve the security management in a company by establishing guidelines and principles. The principles that a company should follow, according to the standard guidelines, includes the services of initiating, implementing, maintaining, and improving information. This sequence of activities leads the company to achieve the main goals of information security management. ISO/IEC 27002:2005 contains best practices of the proper operation of the company, the ways of personal data protection and the legal management of the issue, the support of the information and communication systems security, as well as a short explanation of policies, models and the necessity for conformity.

Apart from the possibility of enhancing the security, the standard ISO / IEC 27002:2005 also supports legal conformity. It stipulates the advising of employees on the reasons and the means of monitoring. The company controls the process of collection and stores employees' data in order to ensure compliance with legal obligations. Moreover, it determines that an official method for discipline should be applied for employees that tend to violate the security policy and business processes. However, the ISO / IEC 27002:2005 can cause certain problems, in order to the security and privacy of employees coexists in a system. The attributes of security do not often coincide with employees' privacy requirements, so that they create contrary needs, such as pseudonymity and identifica-

tion. Moreover, because of the diversity of legal frameworks of countries there could not be a common legal example (Gerber M. and von Solms R., 2008).

However, it seems that ISO / IEC 27002:2005 entails solutions for balancing the competing rights and goals. Instead of an extensive policy it proposes the introduction of context-specific policies and processes for concrete information systems. ISO / IEC 27002:2005 allows the effective management of the security of information systems while providing general guidelines that can assist the administrators to determine the policy in order to maintain a system that provides security and protection of employer and employees' interests and privacy accordingly.

## 6. Conclusions

Monitoring is -per definition - likely to violate employees' autonomy and their right to be free from unjustified intrusion into their workaday life. We tried to lay down how technology could serve both aims: ensuring security and other legitimate rights and interests of the employer while preserving the right of employees to privacy and data protection. Neither the interests of employers nor the privacy rights of employees are absolute values. Conflicting laws, jurisdictional and theoretical approaches reflect not just the contrasting philosophical assumptions of different legal systems but also the inherently ambiguous relationship between property and privacy rights in the contemporary workplace (Findlay and McKinlay, 2003).

It is highly important for a company to specify its real security requirements and to select the appropriate security technology. Usually, risk analysis techniques tend to aim at protecting the security of the enterprise without taking into account even the legally binding limitations concerning employees' data collection and further processing. The commonly used methods in this case is evaluation of the risks an enterprise is confronted with, the legal framework, including the rules and the requirements set by the enterprise itself, the moral and reasonable obligations of the enterprise towards the society, its personnel and its partners (Mitrou and Karyda, 2006).

Employers would also benefit from applying specific use policies for their information and communication systems. These policies should be organized within a wider security management framework, so as to address both the issue of information systems security, especially the insider threat, and, at the same time, provide a fair and lawful monitoring scheme. In this way, employees can have a clear expectation as to what is considered responsible and ethical use of the infrastructure put at their disposal by the employer. Taking into consideration the difficulties to formulate an effective, fair and applicable use policy, the



conflict of employers' legitimate interest to run their business effectively and the employees' legitimate concerns for the protection of their privacy, is all but easy to solve.

## References

American Management Association. (2005). *Workplace e-mail and instant messaging survey*. Retrieved March 2006, from <http://www.amanet.org/research/>

Ball, K. (2006). Expert report: Workplace. In D.M. Wood (Ed.), *Surveillance studies network, a report on the surveillance society for the Information Commissioner (UK)*, Appendices, London, pp. 94-105

Bloom, E., Schachter, M., & Steelman E. H. (2003). Competing interests in the post 9-11 workplace: the new line between privacy and safety. *William Mitchell Law Review*, 29, pp.897-920.

Boncella R.J. (2001), Internet Privacy: At Home and At Work, Communications of AIS, Volume 7 Article 14, online available at: <http://www.washburn.edu/faculty/boncella/INTERNET-PRIVACY.pdf>

Chieh-Ning Lien, Chien-Chia Chen, (2008). Keylogger Defender, UCLA Computer Science Department, Los Angeles, CA 90095, USA, online available at: [http://www.seas.ucla.edu/~chienchi/reports/CS236\\_keydef\\_pp1.pdf](http://www.seas.ucla.edu/~chienchi/reports/CS236_keydef_pp1.pdf)

Commission Nationale de l' Informatique et des Libertés (CNIL), (2002). La cybersurveillance sur les lieux de travail. Paris

Data Protection Working Party (DPWP), (2001), Opinion 8/2001 on the processing of personal data in the employment context. 5062/01/Final.

Desprochers, S., Roussos, A., (2001). The jurisprudence of surveillance: a critical look at the laws of intimacy. Working Paper, Lex Electronica 6(2), Available from: <<http://www.lex-electronica.org/articles/v6-2/>>.

European Commission, (2002). Possible content of a European framework on protection of workers' personal data.

Fazekas, P., (2004). 1984 is still fiction: electronic monitoring in the workplace and U.S. privacy. *Duke Law & Technology Review* 15. Available from: <<http://www.law.duke.edu/journals/dltr/articles/PDF/2004DLTR0015.pdf>>.

Findlay, P. and McKinlay, A. (2003). Surveillance, electronic communications technologies and regulation. *Industrial Relations Journal*, 34(4), 305-314.

Gerber M., and von Solms, R. (2008), Information security requirements – Interpreting the legal aspects, *Computers & Security*, 27, p. 124-135.

Gomes R. and Lapão LV., (2008), The adoption of IT security standards in a healthcare environment. *Proceedings of MIE2008, Studies in Health Technology and Informatics* 136, p. 765–770.

Iglezakis I. (2009), Surveillance of Employees' Electronic Communications in the Workplace: An Employers' Right to Spy or an Invasion to Privacy?, *Socioeconomic and Legal Implications of Electronic Intrusion*, in Politis D., Kozyris P., Iglezakis I. (eds.), *Socio-economic and legal implications of electronic intrusion*, IGI, p. 246-260.

International Labour Office (ILO), (1997). *Protection of workers' personal data*. Geneva.

Klare, E., (1982). *Critical theory and labour relations law*. In: Kairys, D. (Ed.), *The Politics of Law*, New York, pp. 62ff.

Lasprogata, G., King, N., Pillay, S., (2004). Regulation of electronic employee monitoring: identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stanford Technology Law Review* 4. Available from: <[http://stlr.stanford.edu/STLR/Article?04\\_STLR\\_4](http://stlr.stanford.edu/STLR/Article?04_STLR_4)>

Liu Y., Olivier M. S. (2008), Using encryption and trusted third parties to enable data anonymity in the Flocks, *CiteSeerx*.

London Economics (July 2010), *Study on the economic benefits of privacy enhancing technologies (PETs)*, Final Report to The European Commission DG Justice, Freedom and Security.

Mitrou L. & Karyda M. (2006), Employees' Privacy vs. Employers' Security: can they be balanced? *Telematics and Informatics Journal*, 23(3), 2006, pp. 164 – 178.

Mitrou L. & Karyda M. (2009), Bridging the gap between employee's surveillance and privacy protection, œ Gupta M. and R. Sharman(ed.), *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*, Information Science Reference (IGI Global), Hershey-New York 2009, pp. 283-300

Nada M. A. Al-Slamy (May 2008), E-Commerce security, *IJCSNS International Journal of Computer Science and Network Security*, VOL.8 No.5, p 340-344.

Pering T., Want R., Rosario B., Sud S., Lyons K. (2009). Enabling Pervasive Collaboration with Platform Composition, *Proceedings of the 7th International Conference on Pervasive Computing*, Nara, Japan, pp 184 -202.

Phillips, J. D. (2005). Privacy and data protection in the workplace: the US case. In S. Nouwt, B. R. de Vries, & C. Prins (Eds.), *Reasonable expectations of privacy* The Hague, PA: TMC Asser Press., pp. 39-59.

Qadeer M. A., Iqbal A., Zahid M., Siddiqui M. R. (2010), Network Traffic Analysis and Intrusion Detection Using Packet Sniffer, *2010 Second International Conference on Communication Software and Networks*, iccsn, pp.313-317.

Rodota, S. (2004). Privacy, freedom and dignity. *Closing remarks at the 26th International Conference on Privacy and Personal Data Protection*, Wroclaw - Poland

Sagiroglu S., Gurol C. (2009), Keyloggers: Increasing Threats to Computer Security and Privacy, *IEEE Technology and Society Magazine* 28, no.3, p.11-17.

Schultz, E.E., (2002). A framework for understanding and predicting insider attacks. *Computers and Security* 21 (6), 526–531.

Selmi, M. (2006). *Privacy for the working class: public work and private lives* (Public law and legal theory working paper No 222). The George Washington University Law School.

Simitis, S., (1999). Reconsidering the premises of labour law: prolegomena to an EU Regulation on the protection of employees' personal data. *European Law Journal* 5, pp. 45–62.

Stedman R., Yoshida K., Goldberg I. (July 2008), A User Study of Off-the-Record Messaging, *The 2008 Symposium on Usable Privacy and Security* (SOUPS 2008), pp. 95–104.

Suda Y. (2005), Monitoring e-mail of employees in the private sector: a comparison between Western Europe and the United States, *Washington University Global Studies Law Review* 4 (2005), pp. 209-262

UK Information Commissioner, (2003). The Employment Practices Data Protection Code.

Wessels D. (2004), Squid the Definitive Guide, *Reilly Media*, Inc, USA.

# Consent for data processing in e-commerce transactions: UK empirical evidence

---

Stavroula Karapapa &  
Indranath Gupta

---

## Introduction

With the controversy over the *Phorm* advert system<sup>1</sup>, the issue of UK's compliance with the EU requirement on data protection consent has become preeminent. Following several complaints issued in *Phorm*, the Commission announced in 2010 that it has referred the UK to the European Court of Justice for improper implementation of the EU rules on data protection<sup>2</sup>. Part of this referral was the failure of the UK to implement in national law, namely in the Data Protection Act, the definition of consent being as the "freely given, specific and informed indication of a person's wishes"<sup>3</sup>. Besides the judicial timeliness of the issue of consent for data processing, this issue is of paramount importance in the online environment. With expansion of e-commerce, social networking and e-governance, submission of personal data to websites has become an essential prerequisite for taking advantage of any online service. At the same time, possession and processing of personal information represent a key asset for online service providers, as it is an increasingly essential component of their business models in the web 2.0. This creates an issue of major social concern, as control over personal information may deeply affect consumer privacy.

- 
1. Case Ref No 5253/08; B. Johnson, "Outrage as new *Phorm* trial begins", *The Guardian*, 30 September 2008. On April 2011 the Crown Prosecution Service decided not to prosecute BT Group Plc and *Phorm* Inc on the basis of s.s 4.2 of the Code for Crown Prosecutors ('a prosecution would not be in the public interest'). See Crown Prosecution Service, "CPS decides no prosecution of BT and *Phorm* for alleged interception of browsing data", 8 April 2011, available online at <[http://www.cps.gov.uk/news/press\\_releases/116\\_11/index.html](http://www.cps.gov.uk/news/press_releases/116_11/index.html)>, lastly accessible on 9.9.11.
  2. Digital Agenda: Commission refers UK to Court over privacy and personal data protection, IP/10/1215, Brussels, 30 September 2010.
  3. Article 2h of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal* L 281, 23/11/1995 P. 0031 – 0050 (hereinafter referred to as the Data Protection Directive).

Despite the great scholarly attention “the issue of consent for data processing has attracted that has attracted” there is little empirical evidence as to whether commercial websites comply with data protection law in this respect. This paper fills in this gap in literature by laying down the results of an empirical survey, examining the data compliance of 200 websites registered with “.co.uk” domain. The survey primarily assesses whether consent has been legitimately obtained. This assessment ascertains whether the consent expressly includes processing of data for direct marketing purposes, or it is merely some general form of consent towards non-explicit purposes. The survey further examines the way in which consent is obtained from the data subjects. Even though there are many ways to obtain consent in online interactions, for instance, by asking the user to click in a box during registration, such consent is deemed only to be valid if users are given the opportunity to freely “opt in” for receiving commercial communications.

The paper is divided into two main parts. The first part lays down the legislative framework of consent for data processing. Emphasis is given on the requirement that the data subjects should be duly informed about the purposes of data processing before giving out their personal data. The second part outlines the empirical results by reference to the methodology used for their extraction.

## 1. The legislative framework

Personal data should not be processed unless certain conditions are met<sup>4</sup>. Consent in the collection and processing of personal data is a key concept in data protection law. Whereas the requirement of consent features expressly in the Data Protection Act<sup>5</sup>, the meaning of consent in the context of data protection is not defined<sup>6</sup>. Schedule II, s 1, of the Act only stipulates that the lawfulness in the processing of personal data is premised upon condition that the “*data subject has*

---

4. These conditions fall into three categories, namely transparency, legitimate purpose, and proportionality.

5. Data Protection Act, 1998.

6. See European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union, 4 November 2010, COM (210) 609 final, p. 1; The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168 02356/09/EN, adopted on 01 December 2009, p. 3; European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – “A comprehensive approach on personal data protection in the European Union”, Opinion of 14 January 2011, p. 3. See also Commission of the European Communities, Report from the Commission – First

given the consent to the processing.” Directive 95/46/EC, to which the Act gives effect, gives some guidance as to the scope and meaning of consent. Consent is there defined as “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”<sup>7</sup>. Relatively similar is the definition provided by Recital 17 of Directive 2002/58/EC<sup>8</sup> under which “[c]onsent may be given by any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including by ticking a box when visiting an Internet website.” Both these definitions, share three conditions under which consent is valid: it should be *informed*, *specific* and *freely given*.

### ***1.1 The requirement of informed consent for data processing***

Meant to safeguard autonomy and informational privacy, informed consent is given once the user is provided with information about the purpose of data processing when deciding on whether to consent to this processing or not. The crucial consideration is that the individuals should fully appreciate that they are consenting, and to what they are consenting, irrespective of the way by which the consent has been given<sup>9</sup>. This consideration splits down into two requirements. The first is that the purpose of the processing should be directly informed to individuals. For instance, in a website there should be a clear indication of the purposes for which the data of an individual will be processed. For the consent of that individual to be valid, the data subject should be given the option of making an informed choice on the basis of *adequate* information about data processing. As a matter of fact, the Data Protection Act makes a distinction between situations where the data have been obtained directly from the data subject and situations where the data has been obtained otherwise<sup>10</sup>. The Act indicates that the informed character of the consent is essential in establishing fairness in the

---

report on the implementation of the Data Protection Directive (95/46/EC), Brussels, 15 May 2003, COM (2003) 265 final.

7. Article 2h of the Data Protection Directive. Recital 30 of the Directive defines consent as an expression of the will of the data subject.
8. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal* L 201, 31/07/2002 P. 0037 – 0047 (hereinafter referred to as the e-Privacy Directive).
9. Douwe Korff, “Comparative Study on Different Approaches to New Privacy Challenges in particular in light of Technological Developments – A.6 – United Kingdom”, June 2010, European Commission, Directorate General, p. 56.
10. Compare Schedule 1, Part II, Paragraph 2(3) and Schedule 1, Part II, Paragraph 2(1)(b) of the Data Protection Act.

processing of personal data<sup>11</sup>. By virtue of Schedule 1, Part II, Paragraph 2(3)<sup>12</sup>, information should cover at least the identity of the company, the purposes of the processing and any further information. This further information should be necessary with regards to the specific circumstances for which the data is collected, with a view to guarantee fair processing in relation to the individual concerned<sup>13</sup>.

The second requirement for informed consent is the timing of informing individuals on how their data shall be processed. Timing in this context refers to the condition that individuals should be informed about the purposes of processing at the time of the collection of their data. This applies irrespective of the medium or the practical difficulties that may be raised. This emanates from the *Innovations* case<sup>14</sup> where the Data Protection Tribunal found that the collection of data in the context of telephone sales, with the intention of being disclosed to third parties for direct marketing purposes, is not fair if the individuals are not fully informed at the time of data collection. In this case, individuals are “mislead or deceived” and there is no lawful ground for their data being traded in this way. Therefore, data subjects should be aware at the outset of the purposes for which their information will be used so as to be capable of making informed decisions over entering this relationship or not. This is in line with the general rule that fairness<sup>15</sup> in the processing of personal data requires *transparency*, i.e. a clear and express indication of how the data shall be used<sup>16</sup>. Fairness in the processing largely depends on the method by which personal data has been collected. For instance, it is highly unlikely to find fairness in cases where the information has been obtained by

---

11. The processing of personal data can only be fair and lawful once the data subjects have given their consent for this processing. This emanates from Part I of Schedule I of the Data Protection Act, under which: “*Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—E+W+S+N.I. at least one of the conditions in Schedule 2 is met.*”

12. This broadly corresponds to Article 10 of the Data Protection Directive.

13. To qualify as informed, consent should be appropriate to the age and capacity of the individual giving it and to the particular circumstances for each case.

14. *Innovations (Mail Order) Ltd. v. Data Protection Registrar* (Case DA/92 31/49/I), Data Protection Tribunal Decision of 28.9.1993.

15. Paul M. Schwartz & Joel R Reidenberg, *Data Privacy Law: A Study of U.S. Data Protection*, Charlottesville: Michie Law Publishers, 167-71 (1996).

16. The importance of transparency becomes more straightforward in situations involving choice of entering in a relationship. In commercial relationships, this element of choice is more than obvious, since consumers may not wish to enter in such relationship if they do not agree with the terms and conditions relating to the processing of their personal data.

deceiving or misleading potential consumers, namely where consent has not been informed<sup>17</sup>.

## ***1.2 Informed consent in the context of e-commerce***

In the context of electronic communications, consent may be sought either via an opt-in or an opt-out method. Opt-in covers situations where consent is indicated by ticking a box to express agreement to data processing, whereas opt-out refers to where a box may be ticked to indicate objection to data processing (see examples in figures 1 and 3 below). The Information Commissioner's Office (ICO) has distinguished between someone who has been offered the option to object but has not used it, and someone positively confirming their consent by ticking a box<sup>18</sup>. Under the rules incorporated in the Privacy and Electronic Communications Regulations, direct marketing is only legitimate if the recipient has previously indicated consent to receiving such communications. This could take place by actively consenting to the marketing, e.g. by ticking an opt-in box to consent to the marketing, rather than to an opt-out box. Opt-out does not result in valid consent. This rule is subject to limited exceptions. These relate to the use of a "soft opt-in". Soft opt-in includes, for instance, pre-ticked boxes (see figure 2 below); users should un-tick, should they not wish that particular service. A soft opt-in may be used where the data has been obtained in the course of a sale of a product/service to the recipient. It is required that the direct marketing should relate only to similar products and services<sup>19</sup>, and that the recipient has been given a simple means of refusing the use of his/her data for such direct marketing at the time of data collection. If these conditions are met, the difference between the soft opt-in and the opt-out boxes becomes very subtle. So, whereas opt-in is the legitimate way of obtaining valid consent, soft opt-in mechanisms may be also lawful if they fulfil the aforementioned conditions. If consent has been obtained via an opt-out, it is not lawfully obtained.

---

17. This is affirmed by Part II of Schedule I of the Data Protection Act, which provides guidance as to the interpretation of the principle of fairness in the processing of personal data. This section reads that "*regard is to be had to the method by which [personal data] are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.*"

18. <<http://www.ico.gov.uk>>.

19. The application of this condition with respect to «similar products and services only» reflects a purposive approach. This means direct marketing should relate to products and services for which an individual would have a reasonable expectation to receive advertisements or other promotional materials. It is unlikely that such soft opt-in would further cover marketing of other products/services offered by third party companies.



As of May 26, 2011 the UK policy on the use of cookies and similar technologies for storing information has changed to comply with Directive 2009/136/EC. Regulation 6 of the Privacy and Electronic Communications Regulations 2003, which reflects Article 5(3) of the Directive, stipulates that cookies can only be placed on machines where the user has provided their consent.

**Please fill in all the boxes**

Title ☐ Mr. ☐ Mrs. ☐ Ms.

Last Name

First Name

E-mail

☐ I would like to be informed of new products and promotions through Pixmania.com.

☐ I'd like to receive email notifications about Invitation-only shopping on Pixmania.com.

☐ I would like to receive the best offers from PIXmania's partners (special offers, great deals, games and competitions etc.)

In accordance with the IT law of 06/01/1978 (art. 27), you have the right to access and modify all of your personal information

---

**Register your details here**

**Please complete this form**  
All fields marked \* must be filled in.

Email address: \*

Full Postcode: \*

Password: \*

Confirm Password: \*

Address 1:

Address 2:

Address 3:

First Name: \*

Surname: \*

Town:

Telephone number:

County:

Mobile number:

☐ Tick here to confirm that you have read and accepted our [terms and conditions](#)

☐ Tick here if you'd like Exchange and Mart to contact you occasionally with news and offers via email

☐ Tick here if you'd like third party partners to contact you occasionally with news and offers via email

☐ Tick here if you'd like Exchange and Mart to contact you occasionally with news and offers via SMS (please enter your mobile number above)

**conceded. botent**

Type the two words:

Figure 1: examples of opt-in to data processing

## SET UP YOUR ACCOUNT

Please enter your details below.

All the information that you give us is needed to complete the checkout. Topshop will not pass it on to any 3rd parties.

To find out more, please read our [privacy statement](#).

Required fields\*

### YOUR EMAIL ADDRESS AND PASSWORD

Email address: \*

Password: \*

Confirm password: \*

Please note: you need a password in order to track your order progress. Passwords should be at least 6 characters long and include 1 number.

### YOUR NAME

Title: \*

First name: \*

Last name: \*

☒ Please sign me up to receive news on Topshop's latest collections, events and promotion through email and post.

[BACK](#)

[CONTINUE](#)

Figure 2: example of soft opt-in to data processing

Register with us and make your visits to Argos.co.uk even quicker and easier! \* must be completed

First name:*	<input type="text"/>	Security question: <input type="text" value="Select a security question"/>
Email address:*	<input type="text"/>	Security answer:*
Confirm email address:*	<input type="text"/>	Telephone: <input type="text"/>
Password:*	<input type="password"/>	Postcode:*
(min. 6 characters incl. 2 numbers)		Country: <input type="text" value="United Kingdom"/>
Confirm password:*	<input type="password"/>	<input type="checkbox"/> Remember me

By submitting your details, you agree to the use of your personal information as set out in the privacy policy. This includes for the purposes of administering our website services, placing orders, competitions/prize draws and fraud prevention.

You will also be indicating your consent for your details to be used in our marketing programme and receiving marketing information by email, telephone, SMS text message and other electronic messages such as picture messaging, post and fax as explained in the Privacy Policy, unless you indicate otherwise by ticking the boxes below.

☐ NO - I do not want to receive the email newsletter containing all the latest offers, products and competitions, nor to be kept informed about products and services from the Home Retail Group.

☐ NO - I do not want to share my details with carefully selected companies outside of the Home Retail Group for their marketing programmes

*start now*

Name:

Email address:

Postcode:

[create an account](#)

*log in* (if you have already signed up)

Email address:

Postcode:

[login](#)

[Cancel](#) [Register](#)

We will send an email to notify you when you only have a few days left to save on your favourite sofa ranges. If you do not wish to receive such information, please check the box. ☐

Figure 3: Examples of opt-out from data processing

Note that consent may be informed but it may not be specific, as dictated by the European Directives. At the same time, specific consent shall always be informed, as explained below.

### ***1.3 The requirement of specific consent for data processing***

Fairness in the processing of personal data requires that the consent given by individuals is also specific. This means that consent should relate to a defined set of activities about which the individual has been informed at the time of giving consent. The practical significance of the requirement for specific consent is highlighted in situations where the purpose for obtaining or processing the data changes after obtaining user consent. In these cases, the consent is not considered to be valid and any activity related to these data shall be deemed unlawful. There are two issues that need to be addressed in light of specificity of a valid consent: “these are namely, changes to the purposes of data collecting and processing after the time of data collection and the duration of the validity of the consent”.

As to the first issue, changes to the purpose of data collection and data processing after the stage of obtaining user consent mean that the consent cannot any longer be assumed as being specific. Rather, such changes will not be covered by user consent. That would include, for instance, data processing for incompatible secondary purposes. Since consent is not specifically given with regard to these purposes, processing will be hence unlawful<sup>20</sup>.

What is more, the requirement of specificity of consent for data processing further implies that the consent for particular uses of personal data is not perpetual. It lasts up to the point where the purpose of processing changes. This is applicable under two conditions. First, the individual giving consent should have the option to withdraw, and, secondly, the nature of the consent given and the circumstances of data collection and use should be taken into account. Nonetheless, the option to withdraw consent does not affect the validity of data uses that have already been made by virtue of the consent.

### ***1.4 The requirement of freely given consent for data processing***

Consent should also be freely given. This condition has a twofold meaning. First, the individual should be able to actually choose whether they wish to give their consent or not; consent that has been enforced under undue influence or other

---

20. Note however that data processing for historical, statistical or scientific purposes is not considered to be incompatible with the purposes for which the personal data has previously been collected, insofar as suitable safeguards are set in place. See Recital 29 and Article 6(1) (b) of Directive 95/46/EC.

kind of pressure is invalid. For instance, a pre-selected opt-in box could be considered as going against the freedom of choice to consent, despite the fact that choice to unselect is available. This is because the individual's consent is biased and freedom to consent is degraded into extra care in reading the terms and conditions. Secondly, the individuals who have freely given their consent should also should also have the capacity to revoke their consent at any time. In cases where user consent has been given via an opt-in method for a particular service, end users should be given an actual option to opt-out at some later stage in case they do not wish this service any longer. If, for instance, an individual has freely opted in receiving emails for marketing purposes, the email they receive should incorporate an option of opting out of this service. Certainly, there are situations where the provision of a service is conditioned upon consent to the storing of personal information. Arguably, therefore, consent should clearly emanate from the data subject in a way that no doubts exist over his/her agreement, whatever form it takes, oral or written<sup>21</sup>.

For the purposes of the empirical survey, we have translated the legal requirement concerning consent for data processing into a set of variables to test the compliance level of UK websites. Below we analyse the methodology and outcomes of the empirical survey.

## 2. Empirical survey on UK websites

Further to our observation of the legislative framework in relation to consent, this section considers an empirical survey on websites registered in the UK. The empirical survey will be indicative of whether the websites are compliant to the requirement of data protection, especially in relation to consent. A part of this survey is being conducted to observe whether the practices of websites commensurate to the requirement of valid consent, i.e. informed, specific and freely given.

### 2.1 *Method used in empirical survey*

This empirical survey is comprised of two stages. First, we have selected the sample websites, and secondly, the appropriate measures for the websites have been set up to observe their compliance level in relation to valid consent.

---

21. Carey, op. cit. at 39, 74-75; Webster, op. cit. at 39, 26-27; Jay and Hamilton, op. cit. at 7, 150-162. The Data Protection Authorities of the Member States have explicitly shared this view. See Korff, supra at footnote 9, at pp. 36, 74-78. Note, however, that in the UK, the data protection authority indicates that consent maybe implied in certain circumstances. Korff (75) criticises this interpretation as not being fully compliant with the Directive. The latter requires that the data subject's agreement to any processing be 'signified'.

In the context of sample selection, we have looked at two hundred UK websites with sub-domain ‘.co.uk’. As our research focuses on collection of personal data in typical e-commerce services, the two hundred websites are categorised under five headings, namely: *goods, services, informative, news & entertainment* and *mobile, internet & telecom*. Google AD Planner has been the primary source of these websites<sup>22</sup>. In the Google AD Planner, the preliminary search method is through the ‘audience’ option via which one can obtain list of websites<sup>23</sup>. After going through the preliminary audience option, the other parameters required for the survey are the following:

Options	Selection
Geography	United Kingdom (England, Scotland, Wales & Northern Ireland)
Language	English
Ranking Method	Best Match
Domain Suffix	‘.co.uk’

For our survey, the aforementioned selection process provided us with top two hundred websites. Websites in this sample size are well represented under the categories outlined above and provided us with a trend of compliance level to other websites in the context of data protection. The websites have been limited within the geographical boundary of the UK with English as the used language. We chose the ‘best match’ method to get a good representation of all big, medium and small size UK websites. In comparison to other available options, this method is best suited for the purpose of our survey. For instance, if we had used ‘composition index’, we would have got a list of smaller websites. Similarly, if we had used ‘audience reach’, it would have shown us larger websites. In addition, we have left out banking and financial websites as well as websites that are relatively less likely to process personal data. We assumed that banking websites are likely to show a better level of adherence to the consent requirement, while processing personal data. To observe the compliance level of websites, particular practices have been tested, compared and analysed, that directly relate to the consent requirement.

22. Google AD Planner is a free media planner tool that helps companies to advertise and build up their target audience. <<https://www.google.com/accounts/ServiceLogin?service=branding&ltmpl=adplanner&continue=https%3A//www.google.com/adplanner/>> (accessed October 10, 2010) It is a well-known standard service used by major companies for commercial purposes. There are other similar services like Alexa and Comcast.

23. The audience option is available after entering the username and password on the Google AD Planner homepage.

### **3. Consent lost in the complexities of practices by websites**

For our survey, we have looked to the purpose of processing, the method of obtaining user consent and to the degree of freedom attached to the consent given. The identification of user's knowledge has been against the background of specificity and adequacy surrounding the practices of websites prior to processing personal data. Further to the preliminary stage of user's knowledge, there is the issue of communication of information by the website to the user and of the methods adopted by the websites in this regard. In addition, we have investigated the legality of such methods adopted in the context of consent to the purpose of data processing. Further to such investigation, we have also looked at the aspect of user's free will at the point of communicating consent as well as the overall practice of websites in this regard. This empirical survey specifically analysed the consent requirement in relation to direct marketing and advertising communications.

#### ***3.1 Inadequate information provided to data subjects***

The purpose of processing personal data is generally stated in the terms & conditions (hereinafter t&c)/privacy policy, and provides the reason behind collecting personal data in relation to their future use. In the context of valid consent, the purpose of processing should inform the data subject (user) about the exact reason of connecting with the collection of personal data. Further to such specific knowledge, the user should be able to make an informed decision to give his consent freely for such processing.

The sample survey shows that the majority of websites state the purpose of processing in their t&c. Out of the two hundred websites, six have not stated purpose of processing. This constitutes a meagre 3% of the total websites in our survey that do. However, this figure is highly deceptive in the context of communicating information to the data subjects. The figure outlined above merely shows the basic existence of the statements, which apparently talks about the future intention of websites in relation to the processing of personal data. This does not necessarily mean that such intention has been explicit, put forth clearly to the user, and "that it has been clear enough so as to be easily". Although we have not followed a grade system to decipher the adequacy of such information, the empirical survey shows that the statements made by the websites in relation to the purposes of processing are seldom clear and specific.

It follows from such an observation made that there is a broad way of representing purpose of data collection. In some websites, it has been limited to specific purposes, while in others purpose has been rather flimsy. For example, a typical statement on the part of the websites in this regard is that the use of users' per-

sonal data will relate to direct communications and to any other related purpose. Using words like 'any other purpose' is not sufficiently precise, and presents inadequate information as to present and future use. At times, it has been difficult to determine the precise scope of such statements. Since the information provided is not specific, it provides certain difficulties in the context of consent provided by user. First, if the information provided is not specific, then, it has serious bearing on consent given. The previous section shows that data protection regulation requires specific consent for processing. If the purpose of processing is not specific, then the consent can be never specific in relation to such processing. Consent given at the time of data collection may not be valid for a different purpose, since the purpose of processing is not clear. Secondly, if there is inadequate communication of information, the knowledge of the user about the exact purpose of processing personal data is questionable. Thirdly, the adopted practice of inadequate information leaves the user with considerable doubt in relation to the future use of personal data. This practice is against the legal requirement about the free and transparent use of personal data<sup>24</sup>. On top of that, it is debatable whether websites actually abide by such self-proclaimed policy in relation to data processing even if such purpose is specific<sup>25</sup>. Any difference between policy and practice will show up in future transactions with the user. Finally, if the requirement of purpose of processing is unclear, then any communication other than the collection of data may turn out to be illegal on the ground of invalid consent. This brings us to the position to analyse the consent aspect in much more detail.

### ***3.2 Consent doubtful in the background of inappropriate methods***

Not only are the websites obliged to inform the user about processing of personal data, but they are also required to offer to the user effective means to provide consent upon receipt of such information. In the absence of such option, information provided to the user about data processing is of little use. Before going into the details about the websites' practices in relation to consent, and their validity, it would be worthwhile to understand the methods adopted by those websites to facilitate communication of consent in relation to the information provided. In this regard, the websites adopt a wide variety of ways to facilitate consent and as a result, there is no uniformity. To understand the minimum standard practice on the part of a website, the parameter we have considered is one of the most

---

24. Schedule 1: The Data Protection Principles – Part I: The Principles, available at <<http://www.legislation.gov.uk/ukpga/1998/29/schedule/1>>, lastly accessed 12<sup>th</sup> December 2010.

25. Considerable doubt exists because of the use of *Phorm* technology. Websites tend to suppress what they are doing, thereby, going beyond their spoken words in t&c.

popular practices of ticking a box as a sign of providing consent<sup>26</sup>. Instead of ticking a box, another popular way of showing consent is to click the 'button' used for completing the registration process. The act of clicking the button by the user amounts to sign of consent to the t&c. In these cases, there is express written confirmation in the area of the button effectively means that button. This effectively means communicates consent to the websites' conditions. For the empirical survey, we have considered whether websites provide options relating to facilitation of consent communication by following at least either of the two practices, i.e. ticking a box or clicking the button. Based on the outlined above standard practice "out of all websites", the survey shows that 8%, websites fails to provide consent option for the user even after providing purpose of processing in the t&c<sup>27</sup>. It is clear that these websites would be in violation of the consent requirement envisaged under the data protection law. However, the empirical survey observes interesting outcome in relation to the other remaining 92% of websites<sup>28</sup>. Even providing the user with processing purpose, the remainder (92% of websites) have failed to follow the requirements of a valid consent. In the context of appropriate method and as seen in the legislative framework, we have observed their practices in the light of 'opt-in' and 'opt-out'. These considerations specifically relate to marketing communications.

### 3.2.1 Inappropriate method of opt-out followed in large numbers

There are two popular ways of stating processing information for user consent. The method can be broadly categorised under opt-in and opt-out. In the case of opt-in, users expressly tick in a box, thereby, specifically opting in to receive communications. This shows that the websites are going to engage in marketing personal data and that there is adequate information about such processing for the users. On the other hand, opt-out also includes cases where users expressly tick in a box. This tick, however, represents the users' wish to exclude them from receiving any further future communication in relation to direct marketing. Similar to the opt-in method, the opt-out also informs the users about marketing practices in relation to personal data. By adopting these methods, websites do request for consent at the point where user completes the registration process for a particular service or goods.

The following table represents the presentation of information for user consent where a typical example in relation to marketing is given. It shows the where

---

26. This example has been provided under Recital 17 of the Directive on Privacy and Electronic Communications, 2002.

27. On file with the authors.

28. Ibid.



opt-out method adopted by the websites. The numbers under 'no' refer to situations where an opt-in method is in place.

**Table 1:** Is consent to marketing sought via an opt-out method?

		Frequency	Percent
All websites	no	129	65
	yes	71	35
	Total	200	100
goods	no	38	59.4
	yes	26	40.6
	Total	64	100.0
service	no	30	68.2
	yes	14	31.8
	Total	44	100.0
informative	no	19	57.6
	yes	14	42.4
	Total	33	100.0
news and entertainment	no	28	71.8
	yes	11	28.2
	Total	39	100.0
internet, mobile, telecom	no	14	70.0
	yes	6	30.0
	Total	20	100.0

This table shows an interesting balance and clear division in the presentation of information for user's consent in relation to marketing. While seventy-one of two hundred websites follow an opt-out method, the rest present information typically in an opt-in method. The percentage between the two existing methods stands at 35% for opt-out and 65% for opt-in. This percentage shows that a sizeable portion of websites tend to follow the opt-out option and thus, makes the future of such consent controversial due to several reasons. It, however, first, although it is difficult to disagree that opt-in and opt-out provides sufficient information to a particular user in relation to data processing, "there is a difference of approach that a website can take between opt-in and opt-out method, that concern explicit consent and no abjection amounting to consent". While consent is explicit in opt-in, there is no consent present when the user is merely opting out from receiving information from websites. The requirement of explicit consent in the legislative framework shows that it is necessary that the user must give explicit consent

prior to processing of personal data<sup>29</sup>. The Information Commissioners' office has taken up this issue of following opt-out method and it has not recommended opt-out under the best practice method<sup>30</sup>. This clearly shows that opt-out is not an acceptable option in the eye of law. In addition, recent changes in the EU about the cookie policy suggest that the user should explicitly opt-in<sup>31</sup>. Therefore, adoption of the opt-out method is controversial on legal grounds.

Secondly, adopting opt-out method can be controversial on the grounds of transparency in the context of business policy adopted by websites. Data retention for revenue earning may prove to be more beneficial for some websites. Thus, the user may receive an opt-out option instead of an opt-in. Following an opt-out policy is quite dubious on the part of websites, especially when there are multiple options and among them, some are opt-in, while others are opt-out. The table shows an inclination of certain websites categories towards the opt-out method. Websites under 'informative' category in table 1 are mostly using the opt-out method in the context of informing users as well as for further facilitation of communicating consent (42%). Similarly, websites under the category of goods are also equally likely (41%) to follow the opt-out method<sup>32</sup>. Under the informative category, websites, namely social networking, family welfare etc. may be more likely to use personal data for marketing purposes in the future. On the other hand, for websites under the category of goods. What may also prove to be beneficial are future marketing communications. It is interesting to note that some websites are following the correct approach of opt-in instead of opt-out. For example, websites under the category of news & entertainment is less likely (28%) to adopt an opt-out method<sup>33</sup>. It could be the case that they are less reliant on the use of personal data to run their business. On the other hand, their focus may be on the requirement of law; or just by coincidence, that they are following the correct method. Amidst the curiosity and doubt, there is always open the possibility of coincidence in cases of websites following the opt-out method. It is beyond the scope of this survey to have data that suggests the reason that lies behind any decision to adopt either opt-in or opt-out. Whatever may be the reason, websites must engage to make things more transparent.

---

29. Refer to section 1.3. under the legislative framework.

30. This has been said in relation to marketing and failure on the part of the website to provide adequate notice to the user, Guide to data protection < [http://www.ico.gov.uk/for\\_organisations/data\\_protection/the\\_guide.aspx](http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx)> (accessed 10<sup>th</sup> January 2011).

31. Advice on the new cookie regulation < [http://www.ico.gov.uk/for\\_organisations/data\\_protection/topic\\_guides/online.aspx](http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online.aspx)> (accessed June 10<sup>th</sup> 2011).

32. Refer to Table 1.

33. Ibid.

Finally, our concern relates to the contention that these methods would cause confusion, and would mislead the user. Looking at the varied languages used in this regard, one can safely say there is no uniformity, and that lack of uniformity may result in confusion. In this regard, we have already come across such incidences, while explaining the screenshots describing the issues surrounding soft opt-in and opt-out<sup>34</sup>. Conditions in relation to data processing must be clear, and communication of consent must be explicit via the opt-in method to avoid any future claim of deception.

### **2.2.2 Opt-in appropriate method for direct marketing communications**

As a legal requirement, explicit consent is required for sending direct marketing communications<sup>35</sup>. The Data Protection Act provides some interpretative. It is a way of communicating with user whose data has been processed, and includes information about selling products, services and any promotional offers<sup>36</sup>. When the data has been obtained during the sale or negotiation for direct marketing of a product or service, there is an option on the part of the websites to send direct marketing emails for similar products or services. While discussing the legislative framework for direct marketing communications, we have seen that there is a slight exception in this regard. In the absence of explicit consent, websites may still send direct marketing emails. However, such communications will always provide an opportunity to opt-out in future. An individual is well within his rights to prevent processing of personal information for directing marketing. This right, of course, gives the opportunity to opt-out from direct marketing services and, if the user so desires, he is free to inform the data controller<sup>37</sup>. The website, who is the data controller, upon receiving such instruction from the user, is obliged to stop any further direct marketing communication.

This section looks into details about legal requirement in the light of the results obtained in the empirical survey. For such endeavour, we have looked at three different tables dealing with three different aspects. These are namely provision of direct marketing in the t&c, specific consent asked for direct marketing at the

---

34. Refer to section 1.2. above.

35. Under the rules incorporated in the Privacy and Electronic Communications Regulations, direct marketing is only legitimate if the recipient has previously indicated consent to receiving such communications; Marketing <[http://www.ico.gov.uk/for\\_organisations/sector\\_guides/marketing.aspx](http://www.ico.gov.uk/for_organisations/sector_guides/marketing.aspx)> (accessed 10<sup>th</sup> of January).

36. Section 11, Data Protection Act, 1998.

37. Ibid.

point of registration and future opt-out option for the user. For the purpose of analysis, we will first have the description of the relevant points in all the tables.

**Table 2:** Is direct marketing stated in privacy policy?

		Frequency	Percent
All websites	no	52	26
	yes	148	74
	Total	200	100
goods	no	17	26.6
	yes	47	73.4
	Total	64	100.0
services	no	14	31.8
	yes	30	68.2
	Total	44	100.0
informative	no	7	21.2
	yes	26	78.8
	Total	33	100.0
news and entertainment	no	8	20.5
	yes	31	79.5
	Total	39	100.0
internet, mobile, telecom	no	6	30.0
	yes	14	70.0
	Total	20	100.0

Table 2 shows that websites are not always stating their direct marketing policies in the t&c. In fact, fifty-two out of two hundred websites do not actually inform the user about their direct marketing policy, thereby representing about 26% of the total number of websites used in our survey. Out of these, websites belonging to the category of services are least likely (32%) to state the marketing policy in the t&c, while the websites under the category of news and entertainment are most likely (80%) to provide such information in t&c. Apparently concealing direct marketing policy is not against the legal requirement of data protection, and this situation needs further development, alongside the following tables.

**Table 3:** Is specific consent to marketing given?

		Frequency	Percent
All Websites	no	56	28
	yes	144	72
	Total	200	100
goods	no	18	28.1
	yes	46	71.9
	Total	64	100.0
services	no	15	34.1
	yes	29	65.9
	Total	44	100.0
informative	no	8	24.2
	yes	25	75.8
	Total	33	100.0
news and entertainment	no	7	17.9
	yes	32	82.1
	Total	39	100.0
internet, mobile,telecom	no	8	40.0
	yes	12	60.0
	Total	20	100.0

In table 3, we can observe that websites do not always ask for users' specific consent for marketing communications. This table shows that fifty-six out of two hundred websites do not actually inform the user about their direct marketing policy at the point of registering with the service, thereby representing about 28% of the total number of websites used in our survey. Out of these, websites under the category of internet, mobile & telecom are least likely (40%) to ask for consent in relation to direct marketing communications, while websites under the category of news & entertainment (82%) are most likely to ask for such consent at the point of registration. As observed from Table 2, news and entertainment websites are also most likely to state the direct marketing policies in the t&c. In this context. From the following table (Table 4) interesting observations result about the provision of future opt-out options.

**Table 4:** Can you opt out of marketing at later stages?

		Frequency	Percent
All websites	no	56	28
	Yes	144	72
	Total	200	100
goods	no	19	29.7
	yes	45	70.3
	Total	64	100.0
services	no	9	20.5
	yes	35	79.5
	Total	44	100.0
informative	no	10	30.3
	yes	23	69.7
	Total	33	100.0
news and entertainment	no	13	33.3
	yes	26	66.7
	Total	39	100.0
internet, mobile, telecom	no	5	25.0
	yes	15	75.0
	Total	20	100.0

Table 4, shows that fifty-six out of two hundred websites do not actually give the option to the user to opt-out later, thereby, representing about 28% of the total number of websites used in our survey. Out of these, interestingly, news and entertainment websites are least likely (34%) to give opt-out option at a later date, while websites providing services are most likely (80%) to give opt-out options in the future. When compared with table 2 & 3, news and entertainment websites are most likely to state direct marketing policy in the t&c and ask for specific consent for direct marketing. However, at the point of giving future opt-out options, they are least likely to give any such opportunity. On an overall note, it is evident from all, three tables that websites, which are not stating the direct marketing policies in the t&c, are least likely to ask for specific consent at the point of registration, and are also least likely to give opt-out options later. We will now consider other categories to do individual analyses.

Starting with websites under goods, it is observed that about 27% (table 2) of them do not state the direct marketing policies in the t&c. However, 72 % (table 3) of them ask for specific consent at the point of registration. In the context of

giving options to opt-out later, about 71% (table 4) of such websites do give such opportunity to the user. This reveals that the percentage of websites under goods that do not state the direct marketing policies in t&c (27%) are also least likely to ask for specific consent at the point of registration (28%= 100-72), and are equally unlikely to provide any future option to opt-out (29%= 100-71).

Moving on to services, it is observed that about 32% (table 2) of such websites do not state the direct marketing policies in the t&c, while 66% (table 3) actually ask for specific consent at the point of registration. In the context of giving the opt-out options later, 80% (table 4) of such websites do give such opportunity. This again confirms opportunity what we have seen in the case of goods, although to a relatively lesser extent.

In the case of the informative category, about 22% (table 2) of the websites do not come up with direct marketing policies in the t&c, while 76% (table 3) actually ask for specific consent. On the other hand, 70% (table 4) actually give the opportunity to opt-out later. The websites under informative category also reveal similar trends observed for websites under the goods and services category.

For the category of internet, mobile & telecom, 30% (table 2) of the websites do not mention their direct marketing policy in their t&c, while 60% (table 3) ask for specific consent at the point of registration process. In the context of opting out, 75% (table 4) do give an opportunity to opt-out later. Here, also, the trend, as outlined above, continues.

There seems to be a general trend, even though with varying degrees that websites are least likely to give opt-out option at a later stage, if they fail to mention the direct marketing policy in the t&c (tables 2, 3 & 4). The only exception seems to be the news and entertainment category. However, the problem remains, since the majority of them do not give the option to opt-out later. From the analyses presented above, for transparency and fairness, there should be adequate information for the user about the future intention of websites in relation to use of personal data for direct marketing<sup>38</sup>. This practice is not transparent and far from being fair, since this is the only way for the user to bring an end to receiving commercial communications. On top of that, if the user is not aware of direct marketing policies at initial stages, then the situation becomes even more difficult. To be transparent in relation to data protection policies, the user needs information about direct marketing in the first place. This enables the user to decide at the outset about whether or not he/she should enter into a relationship with a particular website. Even if the website gives future opt-out option, it is unthinkable

---

38. Use of *Phorm* technology provides us with an example of lack of transparency in data processing.

that the website will take the users' consent for granted in relation to direct marketing. In addition, there are cases when websites do not provide opt-out option adequately at a later stage. This makes the issue of informing the user about direct marketing at the initial stages even more important. In relation to these websites, if the user receives direct marketing communications later, one may argue that there has been no information provided about direct marketing at the point of entering into the contract. As a result, in the absence of information, no consent can be associated with the receipts of such direct marketing communications.

There may be further argument that websites, not stating the way to opt-out, are the websites that do not engage in direct marketing communications. These should be the websites that simply do *not* process personal data for direct marketing. While this may be the ideal situation, it will take a lot of persuasion to believe that not stating the direct marketing policies in the t&c, and not providing users with opt-out instructions, will automatically guarantee non-receipt of future direct marketing communications. This brings us to the last segment where we will observe the involvement of free will in the consent.

### ***2.3 Consent devoid of free will***

In this section, we will observe the degree of compulsion and the involvement of free will on the part of the user in the background of marketing emails. Thus, we observed the issue of free will in relation to consent from three aspects: isn't this the same, δnλ. "marketing options that are pre-selected and marketing options that must be selected by the user to proceed and complete the registration process. We have analysed to what extent users give consent against their free will as well as the presence of enough opportunities to express free will. To start with, we will examine the table, which shows the options that are pre-selected prior to users' consent.



**Table 5:** Are some options pre-selected?

		Frequency	Percent
All websites	no	109	55
	Yes	91	45
	Total	200	100
goods	no	37	57.8
	yes	27	42.2
	Total	64	100.0
services	no	22	50.0
	yes	22	50.0
	Total	44	100.0
informative	no	15	45.5
	yes	18	54.5
	Total	33	100.0
news and entertainment	no	25	64.1
	yes	14	35.9
	Total	39	100.0
internet, mobile & telecom	no	10	50.0
	yes	10	50.0
	Total	20	100.0

Table 5 shows that websites are most likely to pre-select options (45%). The figure shows that for every two websites, it is most likely that one will have the options pre-selected. Websites under the informative category mostly pre-select options (55%), while they are closely followed by websites under the category of services (50%) and internet, mobile & telecom (50%). There is a contentious issue at this stage, which questions the fundamental wisdom of pre-selecting options and has been considered after looking at the other tables. Although giving a broad representation of how many times options are pre-selected, this table does not show the instances of pre-selected marketing options. For this, we must observe the figures of the following table.

**Table 6:** Is consent to marketing preselected?

		Frequency	Percent
All Websites	no	133	66
	Yes	67	34
	Total	200	100
goods	no	40	62.5
	yes	24	37.5
	Total	64	100.0
services	no	30	68.2
	yes	14	31.8
	Total	44	100.0
informative	no	20	60.6
	yes	13	39.4
	Total	33	100.0
news and entertainment	no	29	74.4
	yes	10	25.6
	Total	39	100.0
internet, mobile, telecom	no	14	70.0
	yes	6	30.0
	Total	20	100.0

Table 6 shows that, on an overall note, 34% of websites actually pre-select marketing options, while 66 % refrain from such act. Websites under the category of informative are most likely to pre-select the marketing options (40%), while the websites under news and entertainment are least likely to select such option (26%). A comparison of tables 5 & 6 shows that when the options are pre-selected, one third of such websites would have such options pre-selected for marketing (34% of 91 = 30 websites). Further analyses of pre-selecting option of marketing under various categories give us the following result.

In the case of websites under the category of goods, out of 27 pre-selected options (table 5), 24 times (table 6) they are pre-selected for the purpose of marketing, which gives us a staggering proportion of 88%. Under the category of goods, it is highly likely that whenever the options are pre-selected, they would be for marketing. By drawing similar comparisons (tables 5 & 6), we observe the proportion of pre-selected marketing options for Services, Informative, News & Entertainment and Internet, Mobile & Telecom. They are: 64% (14 out of 22) for Services, 72% (13 out of 18) for Informative, 71% (10 out of 14) for News

& Entertainment and 60% for Internet, Mobile & Telecom (6 out of 10). Whenever options are pre-selected, these figures show a higher trend of pre-selecting options for marketing by websites under all categories. Further comparison of tables (1&6) gives us interesting result. Previously, under table 1 furnishes interesting results we have observed that websites under informative are most likely (42%) to use the opt-out method, while asking for user consent. Table 6 shows that this is the most likely category to pre-select options for marketing. It seems these are the websites, which tend to use for less transparent policies, while processing personal data.

This brings us to the question of the policy to pre-select options, especially by pre-selecting marketing options. One might question the legal effect of such an act, since the user is at liberty to un-check the boxes, which have been pre-selected. This is rather easy in an online environment. It also questions the wisdom behind pre-selecting marketing options. As we see it, there are certain problems associated with such an act. First, one may argue that websites tend to simplify the procedure and in the process, pre-select the options on behalf of the user. In order to speed up the registration process, they perform such, act. However, we must question the intention, since selecting or de-selecting a box is not a labourious job. If the user has successfully managed to register for the service offered by the website, then he/she should easily sail through the option by selecting a box. By pre-selecting the option of marketing, the website is creating an obstacle in the exercise of free will and, thus, encroaching upon the freedom of the user. To make things more transparent the website can easily leave that marketing option un-selected, and let the user decide by using his/her free will. In addition, we have also observed that, in certain instances, websites make the selection of marketing option compulsory, although they are less in number (7% of our sample)<sup>39</sup>. In these cases, it is obvious that the consent is not valid. Secondly, if the website has pre-selected the marketing option, it has done so without the website user's consent. The user had never asked to act on his/her behalf and communication in the context of such selection may be contentious in the absence of valid consent. Finally, in the context of transparency, there may be further confusion in the mind of the user. For example, it is evident from our survey that in the case of multiple options, some of the options are pre-selected, while others are not. Under these circumstances, the issue of pre-selecting marketing options is highly questionable when it is not difficult or labourious to show consent by clicking a box.

---

39. On file with the authors.

## Conclusion

Consent for data processing is a key requirement of UK data protection law. To comply with this requirement, websites should inform individuals at the outset to which activities in particular they are providing their consent. Empirical evidence indicates that this requirement is not fully met. Our survey of 200 websites under the “.co.uk.” domain suggests that websites seldom meet the requirements for informed and specific consent in relation to data processing. Whereas in their great majority websites provide individuals with information as to the purposes of data collection, a good percentage of them do not state purposes of direct marketing in their privacy policies. Those websites also fail to provide individuals with the specific purposes for which their data are going to be processed; this means that, if individuals consent to this kind of data processing, consent is not going to be specific and, hence, not valid. Websites that do not state the direct marketing policy in the terms and conditions, are highly unlikely to meet the requirement for specific consent in relation to the marketing purposes at the registration stage. What is more, the method of obtaining consent is questionable on the ground of legitimacy; some websites do not seek consent for data processing at the registration stage. A significant number of websites have set opt-out instead of opt-in – mechanisms for the receipt of advertisements, and only a half of those websites provides users with the opportunity to opt-out from receiving promotional materials at a later stage. This means that the requirement for informed and specific consent for data processing is not fully respected. In some cases, the option of marketing is pre-selected and this encroaches upon the user freedom to consent; this becomes more problematic where the selection of marketing option is compulsory. Transparency and fairness in data processing could be better achieved, should websites inform individuals about their marketing policies at the outset and were more cautious in the application of opt-out mechanisms.

# **Personal data protection in the era of cloud computing new challenges for European regulators**

---

---

**Panagiotis Kitsos & Paraskevi Pappa**

---

---

## **1. Introduction**

It is said that we are entering in an era of a new technological revolution in the sector of information and communication technologies. The emergence of cloud computing services raises several concerns related to the protection of personal data and privacy. which might include sensitive information is transmitted, processed, and stored in remote places .

The responsibility to secure this information falls into the hands of the hosting company. It is very important to determine the role of controllers and processors, to examine how much control and involvement over their personal data individuals have, how does the host company secure this data from possible breaches and which law applies in the clouds.

Our goal is to address these important data protection and privacy concerns within the relevant current European union legal framework and determine whether it can be the adequate response to these concerns.

## **2. What is cloud computing**

The term “cloud computing”<sup>1</sup> is a term that has long been debated and described by IT specialists and fallen into hype. Phrases like “the Cloud is the Computer.”<sup>2</sup> have made their way through numerous discussions on the exact definition of the term.

---

1. The term «cloud» is used as a metaphor for the Internet, based on a cloud drawing used in the past to represent the telephone networks.

2. McFedries P. “The cloud is the computer”, IEEE Spectrum, Online, August 2008. Electronic Magazine, available at <http://www.spectrum.ieee.org/aug08/6490>. We should be careful though, when we define the “cloud as the computer”, since it is possible to underestimate the inherent security and privacy risks that cloud technologies entail. See also Fingar, P. (2009). in “Cloud computing set to unleash a perfect storm in business”, who states: “In short, the cloud is the Real Internet, or what the Internet was really meant to be in the first place: an endless computer made up of networks of networks of computers. Even shorter: the Cloud is

It has been characterized as a result of the ubiquitous broadband access which is “becoming a platform for computing –vast, interconnected virtual supercomputer”.<sup>1</sup>

The National Institute of Standards and Technology, Information Technology Laboratory NIST has defined “cloud computing” as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”.

Further more both in National Institute’s of Standards and Technology, definition of “cloud computing”<sup>2</sup> and the European Network and Information Security Agency’s (ENISA)<sup>3</sup> report on “Cloud Computing”<sup>4</sup> three main categories of cloud computing are defined:

1. Software as a service (SaaS): which is software offered by a third party provider, available on demand, usually via the Internet configurable remotely. Examples include online word processing and spreadsheet tools, CRM (Customer relationship management)<sup>5</sup> services and web content delivery services (Salesforce CRM, Google Docs, etc). So anyone of us with a simple and even cheap computer with limited storage capacity or with a smartphone connected to the Internet or a company network, is able download or upload data from the cloud.
2. Platform as a service (PaaS): allows customers to develop new applications using APIs (Application Programming Interface)<sup>6</sup>. The platforms offered include

---

the Computer.” [http://www.cordys.com/ufc/file2/cordyscms\\_sites/download/6f5f4d1cfe8be9d78d972fa808d8702c/pu/cordial\\_fingar.pdf](http://www.cordys.com/ufc/file2/cordyscms_sites/download/6f5f4d1cfe8be9d78d972fa808d8702c/pu/cordial_fingar.pdf)].

1. Cavoukian A. «Privacy in the clouds», White Paper on Privacy and digital identity: implications for the internet, [www.ipc.on.ca/images/Resources/privacyinthecLOUDS.pdf](http://www.ipc.on.ca/images/Resources/privacyinthecLOUDS.pdf).
2. Mell, P, Grace T. “The NIST Definition of Cloud Computing”, <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>.
3. European Network and Information Security Agency, is as a body of expertise, set up by the EU to carry out very specific technical, scientific tasks in the field of Information Security. <http://www.enisa.europa.eu/about-enisa>.
4. Catteddu D. and Hogben G., “Cloud Computing: benefits, risks and recommendations for information security” [http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at\\_download/fullReport](http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport).
5. The management of a company’s interactions with customers, clients and sales prospects.
6. It serves as an interface between different software programs and facilitates their interaction, similar to the way the user interface facilitates interaction between humans and computers. <http://en.wikipedia.org/wiki/API>.

development tools, configuration management, and deployment platforms. Examples are Microsoft Azure, Force and Google App engine, Youtube.

3. Infrastructure as service (IaaS): provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API. Examples include Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live Skydrive and Rackspace Cloud.<sup>7</sup>

Clouds may also be divided into:

- a) public: available publicly where any organisation may subscribe
- b) private: services built according to cloud computing principles, accessible only within a private network

Simply put, in the field in the cloud any computer connected to the Internet is connected to the same pool of computing power, applications, and files<sup>8</sup>. Cloud computing services exist in many variations, including data storage sites, video sites, tax preparation sites, personal health record websites, photography websites, social networking sites, and many more.<sup>9</sup>

So users can store and access personal files such as music, pictures, videos, and bookmarks or play games or do word processing on a remote server rather than physically carrying around a storage medium such as a DVD or thumb drive. Those of us use web-based email such as Gmail, Hotmail, Yahoo, are making use of cloud email servers as well.

Cloud Computing Service Providers insist that cloud computing is the future in computing applications.

The advantages for users of cloud computing applications are many since any information stored locally on a computer could be stored in the cloud e.g (a). the ability to store more data than a personal computer can available at very low - or zero - cost<sup>10</sup> (b). freedom from having to deal with upgrades and security issues, (c). It allows users to connect from a remote place even without their computer,

---

7. Infrastructure as a Service (IaaS) provides data center, infrastructure hardware and software resources over the Internet, such as server, operating system, disk storage, database, and/or messaging resources.

8. [http://en.wikipedia.org/wiki/Cloud\\_computing](http://en.wikipedia.org/wiki/Cloud_computing).

9. Gellman R., "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing". study prepared for the World Privacy Forum February 23, 2009 [http://www.worldprivacyforum.org/pdf/WPF\\_Cloud\\_Privacy\\_Report.pdf](http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf).

10. Leslie Harris, Perils in the Privacy Cloud (2009) ABC News, 15 Sep 2009 <<http://abcnews.go.com/Technology/AheadoftheCurve/privacy-evaporates-computingcloud/Story?id=8573715&page=1>>.

(d). users do not have to purchase or maintain specific hardware and software applications since they simply rent these services . You pay for what you use and the amount of time you use it. (e). The users do not have to be afraid of possible loss of data due to a stolen or lost computer, cd or flash drive.<sup>11</sup>

The economic benefits for both cloud computing users and national economies can be significant.

According to a report written by the Centre for Economics and Business a widespread adoption of cloud computing in Europe's five largest economies (France, Germany, Italy, Spain and the UK) has the potential to generate over €763 billion of cumulative economic benefits over the period 2010 to 2015.<sup>12</sup>

### 3. Privacy and Data Protection Concerns

Cloud computing though raises strong concerns among privacy advocates. It is pointed out that users, by uploading and storing their data with programs hosted on someone else's hardware, lose a degree of control over their personal information. The responsibility for protecting that information from hackers and data breaches then falls into the hands of the hosting company rather than the individual user.<sup>13</sup> This triggers a series of legal problems on user's privacy and confidentiality risks such as sharing of information collected without consent and weaker privacy protection laws in the country where data centers are.

In a letter to the Federal Communications Commission (FCC), David Vladeck, director of the Federal Trade Commission (FTC) Bureau of Consumer Protection, notes that "the ability of cloud computing services to collect and centrally store increasing amounts of consumer data, combined with the ease with which such centrally stored data may be shared with others, create a risk that larger amounts of data may be used by entities in ways not originally intended or understood by consumers."<sup>14</sup>

---

11. See for the benefits of Cloud computing «Above the Clouds: A Berkeley View of Cloud Computing» by Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. Technical Report EECS-2009-28, EECS Department, University of California, Berkeley.

12. Centre for Economics and Business Research, "the cloud dividend: Part One -The economic benefits of cloud computing to business and the wider EMEA economy France, Germany, Italy, Spain and UK" <http://uk.emc.com/collateral/microsites/2010/cloud-dividend/cloud-dividend-report.pdf>.

13. <http://www.privacyrights.org/ar/cloud-computing.htm>.

14. FTC to examine cloud computing privacy concerns <http://homelandsecuritynewswire.com/ftc-examine-cloud-computing-privacy-concerns>.



He added that the FTC is “considering cloud computing and identity management as part of a broader initiative to re-examine various models to promote consumer privacy.”<sup>15</sup>

Robert Gellman, a Privacy and Information Policy consultant, has produced an influential report for World Privacy Forum on the implications for the privacy of personal information and for the confidentiality of business and governmental information.

In his document, he identifies the multiple and complex privacy and confidentiality issues that may arise by cloud computing services.

In particular, he describes a number of data privacy concerns in Cloud environments such as:

(a) the user’s privacy and confidentiality risks derived from the terms of service and privacy policy established by the cloud provider since many users are not aware of the details set out in these terms or of the consequences of sharing information with a cloud provider, (b) the privacy and confidentiality rights, obligations, and status that may change when a user discloses information to a cloud provider, (c) the consequences that could, disclosure and remote storage, have for the legal status of or protections for personal or business information, (d) the effects on the privacy and confidentiality protections of information and on the privacy obligations of those who process or store the information, since any information stored in the cloud eventually ends up on a physical machine owned by a particular company or a person located in a specific country, may be subject to the laws of the country where the physical machine is located, (e) the user’s information that moves from jurisdiction to jurisdiction, from provider to provider, or from machine to machine, (f) the disclosure of users records to government agents, (g) whether electronic communications laws apply to cloud computing communications or apply differently to different aspects of cloud computing.

These are only some of the concerns raised in relation to cloud computing services and cloud computing is nowadays one the top issues for privacy advocates.

#### **4. Regulatory challenges**

A number of concerns need to be addressed within the framework of European Law for Data Protection.

Peter Hustinx, the European Data Protection Supervisor, in a speech given in 2010 in the Third European Cyber Security Awareness Day, has defined a number

---

15. Id.

of challenges for European regulators such as the determination of responsibilities, the determination of the applicable law, the problems arising from international data transfers, the need of a more effective personal data protection laws in the new technologically advanced environment and the issue of protection to users of cloud computing services, who use them for purely personal purposes.<sup>16</sup>

#### ***4.1 Determination of responsibilities***

The determination of responsibilities in the cloud computing environment can be examined under the light of Directive 95/46/EC which provides obligations on the entities that process data as data controllers. Fewer obligations are imposed on data processors, entities that are 'entrusted' by controllers to process data.

In Hustinx's opinion, even when cloud providers play a mere "processing" role, they will have to engage in a very close cooperation with their clients to ensure that controllers are in a position to fulfil their data protection obligations.

The role of Data Controller and Data Processor is particularly important in the determination of the liability of the parties involved in the process of personal data. The determination of the person responsible for compliance with data protection provisions is directly related to which national laws apply and which data protection authorities can effectively supervise data processing operations.<sup>17</sup>

In Article 29 Data Protection Working Party's Opinion 1/2010 on the concepts of "controller" and "processor" it is stated that the 'processor' "plays an important role in the context of confidentiality and security of processing as it serves to identify the responsibilities of those who are more closely involved in the processing of personal data, either under direct authority of the controller or elsewhere on his behalf".

---

16. Hustinx P. «Data Protection and Cloud Computing under EU law», speech delivered by Peter Hustinx at the Third European Cyber Security Awareness Day, Brussels April the 13th 2010. <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/SA2010>. See also the analysis of Balboni P., "Data Protection and Data Security Issues Related to Cloud Computing in the EU" (August 18, 2010). ISSE 2010 Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe Conference 2010; Tilburg Law School Research Paper No. 022/2010. Available at SSRN:[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1661437](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1661437).

17. Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of «controller» and «processor» available [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf).

It is very important to distinguish between ‘controller’ and ‘processor’ in order to distinguish between those who are responsible as controller(s) and those that are only acting on their behalf.

According to Directive 95/46/EC the ‘controller’ is “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law”.

The ‘processor’ “shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller”.

The application of these definitions though to the cloud-computing environment is a rather difficult task .

On December 2010, the EU Article 29 Data Protection Working Party adopted Opinion 8/2010 on the territorial application of EU Data Protection Directive 95/46/EC and the national data protection laws transposing the Directive.<sup>18</sup>

The Opinion emphasises the complexity of the issue in the cloud computing environment stating that even if the exact place where data is located is not always known and it can change in time, this is not decisive to identify applicable law.

According to Opinion “it is sufficient that the controller carries out processing in the context of an establishment within the EU, or that relevant means is located on EU territory to trigger the application of EU law...”.

As stated in the Opinion the specification of applicable rules is related to the identification of the controller and to the activities that take place at a certain level.

When the user of the cloud service is a data controller, for example when a company uses an agenda service on-line to organize meetings with clients in the context of the activities of its establishment in the EU, EU law will be applicable on the basis of Article 4(1)a.<sup>19</sup>

---

18. Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, 16 December 2010, WP179, [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf).

19. The company should make sure that the service provides for adequate data protection safeguards, notably with regard to the security of personal data stored on the cloud. It will also have to inform its clients of the purpose and conditions of use of their data.

In some circumstances, the data controller can also be the cloud service provider when, for example, it provides for an agenda on-line where private parties can upload all their personal appointments and it offers added value services such as synchronization of appointments and contacts. If the cloud service provider uses means<sup>20</sup> in the EU, it will be subject to EU data protection law on the basis of Article 4(1) c.

#### **4.2 Which law applies?**

The determination of the applicable law is a key issue since in the cloud computing environment, personal data are processed and stored on servers in several places around the world<sup>21</sup>, so the application of the provisions of the Directive 95/46/EC is becoming a complex issue.

Regarding the territorial application of Directive 95/46/EC article 4 of the Directive 95/46/EC requires that each Member State should apply the national provisions to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State.

Article 29 WP in its Opinion 1/2008 on data protection issues related to search engines<sup>22</sup> has explained the concept of the “establishment” stating that “an establishment” implies the effective and real exercise of activity through stable arrangements, adding that the legal form of the establishment – a local office, a subsidiary with legal personality or a third party agency – is not decisive. Also, on the requirement that the processing operation should be carried out “in the context of the activities” of the establishment, the Opinion Clarified that means

---

20. It could include more specific equipment e.g. if the service uses calculating facilities, runs java scripts or installs cookies with the purpose of storing and retrieving personal data of users. The cloud service provider will then have to provide users with information on the way data are being processed, stored, possibly accessed by third parties.

21. As Viviane Reding wrote in, the Wall Street Journal, “a UK resident who creates an online personal agenda could use software hosted in Germany that is then processed in India, stored in Poland and accessed in Spain”. See Reding V., “The Digital Forecast Is Cloudy European consumers need protection against misuse of their information in the online»cloud». <http://online.wsj.com/article/SB10001424052748703555804576101591825228076.html> and [http://ec.europa.eu/commission\\_2010-2014/reding/pdf/news/cloud\\_en.pdf](http://ec.europa.eu/commission_2010-2014/reding/pdf/news/cloud_en.pdf).

22. See Article 29 Data Protection Working Party's opinion 1/2008 on data protection issues related to search engines; available at: [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2009\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm).

that the establishment should also play a relevant role in the particular processing operation.<sup>23</sup>

When the controller is established on the territory of several Member States, then he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable. This actually means that the establishment of the controller is determinative for the applicable national law and “possibly for a number of different applicable national laws and the way in which they relate to each other”.<sup>24</sup>

Furthermore the same provisions apply both when the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law and where the controller is not established on Community territory, but for purposes of processing personal data makes use of automated equipment (e.g., datacenters, servers, etc.) situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.<sup>25</sup>

European Data Protection Supervisor, Peter Hustinx, in his speech on “Data Protection and Cloud Computing under EU Law”, also stated that: “(a) A cloud provider established in the EU – or acting as processor for a controller established in the EU – will in principle be ‘caught’ by the EU law. (b) A cloud provider which uses equipment (such as servers) in an EU Member State – or acting as a processor for a controller using such equipment – will also be caught. (c) A cloud provider in other cases – even if it mainly and mostly targets European citizens – would not be caught by EU law”.

Nevertheless, as a last comment he added that, given that the Directive is in the process of being reviewed, the amendments directed to ensure that Cloud Service

---

23. Id.

24. Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of «controller» and «processor» available: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf).

25. Article 4 par. 1 (c) of the Directive 95/46/EC see also WP 29 Opinion 1/2008 on data protection issues related to search engines; available at: [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2009\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm). which states that “Search engines that use equipment on the territory of a Member State (EEA) for the processing of personal data also fall under the scope of that Member State’s data protection law. A Member State’s data protection law still applies where the controller[...] for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community”.

Providers that target EU citizens “do not escape the application of EU law” may be considered.<sup>26</sup>

### ***4.3 International data transfers***

Closely related to the issue of the applicability of law is the problem of international data transfers.

According to Directive 95/46/EC, transfers of personal data to third countries without an adequate level of protection are prohibited.<sup>27</sup> By way of derogation from Article 25 Member States shall provide that a transfer of personal data to a third country which does not ensure an adequate level of protection may take place on condition that the data subject has given his consent or the transfer is necessary for the performance of a contract between the data subject and the controller or between the controller and a third party, or the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims or the transfer is necessary in order to protect the vital interests of the data subject, and so on.<sup>28</sup>

Moreover, Directive 95/46/EC allows a Member State to authorize a transfer or set of transfers to a ‘non-adequate’ third country ‘where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. The provision specifies that ‘such safeguards may in particular result from contractual clauses’.<sup>29</sup> Article 26(4) also gives a power to the Commission, acting in accordance with the procedure laid down in Article 31, to decide that certain standard contractual clauses offer the sufficient guarantees envisaged in Article 26(2). Also an exception applies if the data controller provides adequate safeguards for the protection of personal data: for example, enter into a contract with the recipient of the data ensuring that the data will remain adequately protected.<sup>30</sup>

---

26. Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, in her speech “The reform of the EU Data Protection Directive: the impact on businesses European Business Summit Brussels, 18 May 2011, noted that this proposal would be one of her priorities in reforming the current data protection framework.

27. Article 25 par. 1 Directive 95/46/EC.

28. Article 26 par. 1 Directive 95/46/EC.

29. Article 26 par. 1 Directive 95/46/EC.

30. Working Party article 29 Working Document “Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive” [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf).

According to Hustinx the problem is that these rules rely on a definition of data transfer from ‘point to point’. They require having a contract, a Model Contract for the transfer of personal data to third countries and sometimes a notification to the authority for each transfer to a country where the legal framework is not adequate.

In practice this is very difficult to implement, particularly in cloud computing which is characterized by a continuous transfer of personal data.

Other solutions, such as Safe Harbor principles, are no better in the cloud computing environment as the personal data moves to different countries and between several companies.

The solution according to Hustinx could also be found in the context of the review of the Directive with the introduction of an extended responsibility for controllers with respect to data transfers. Also, the adoption of Binding Corporate Rules<sup>31</sup> by multinational companies to ensure an adequate level of protection for the intra-group transfers of personal data from a country in the EU or the European Economic Area (EEA) to a third country, seems to be an effective solution as well in the cloud computing environment.

#### *4.4 Efficiency of EU regulatory framework*

The overall goal to ensuring effective personal data protection in cloud computing environment is very important.

Article 29 WP has published a paper in 2010 called “The Future of Privacy”<sup>32</sup> in which proposes the introduction of “Accountability” principle and “Privacy by Design” principle.

The “Accountability Principle” is a provision included in the new legislative framework pursuant to which data controllers Data controllers should have in

---

31. See the toolkit on Binding Corporate Rules (BCRs), issued the Article 29 Working Party on 2008 aimed at promoting them as a mechanism for transferring data to countries without an adequate level of data protection. The toolkit includes: (1) a table highlighting the elements and principles to be found in BCRs [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf); (2) a document setting up a framework for the structure of BCRs, [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_en.pdf); and (3) a revised version of the FAQs on BCRs, [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp155\\_rev.04\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp155_rev.04_en.pdf).

32. Article 29 Working Party “The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data” [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf).

place the necessary internal mechanisms to demonstrate compliance to external stakeholders, including national data protection authorities and would also remain accountable and responsible for the protection of personal data for which they are controllers, even in the case the data have been transferred to other controllers outside the EU.

The “Privacy by Design” principle obliges technology designers and producers as well as data controllers to take technological data protection into account already at the planning stage of information-technological procedures and systems. Providers of such systems or services as well as controllers should demonstrate that they have taken all measures required to comply with these requirement.

The introduction of “Privacy by Design” will also emphasize the need to implement privacy enhancing technologies (PETs), ‘privacy by default’ settings and the necessary tools to enable users to better protect their personal data (e.g., access controls, encryption) in products and services provided to third parties and individual customers (e.g. WiFi-Routers, social networks and search engines).

As Hustinx points out, “in the context of cloud computing services, this means that controllers and processors would have to demonstrate that they have taken all the necessary measures to ensure that data protection rules and principles are complied with. This approach would also be very interesting where personal data are entrusted to providers in third countries”.

#### ***4.5 Protection of household activities.***

The protection of household activities in the cloud under EU law is also a matter that remains to be answered.

The transfer of personal data, such as the storage of pictures and calendars (which usually are stored on local desktops), to data centers that are considered as located in the cloud raises the question whether the cloud provider is covered by the EU data protection law.

Article 3 of Directive 95/46/EC excludes from the scope of application of the Directive data processing carried out “by natural persons in the course of a purely personal or household activity”.

If the information uploaded to the cloud is not covered by the Directive because it is information of a personal nature, then the processing activities that are carried out on behalf of the individuals involved might not be covered either.

This gap in the protection of end-users is definitely an obstacle to the objectives of European Union to protect the fundamental right to privacy and data protection.



So, cloud computing service providers when offering services to a private individual should be required to provide certain safeguards regarding the security, and the confidentiality of the information uploaded by users, regardless of whether their client is a data controller or an end user.

## 5. Conclusions

Current European data protection regulatory framework seems rather weak to adequately address privacy concerns related to cloud computing .

Issues such as applicable law, international data transfers, definition of the responsibilities of data controllers and data processors may have to be readdressed in the context of cloud computing services.

The expected revision of Directive 95/46/EC should take into account all the developments in the Information and Communication Sector and provide a solid legal framework for the protection of personal which is an absolute precondition for cloud computing services to develop and boost the economy across Europe.

Not only consumers, but small and medium enterprises are the ones to benefit most from an adequate legal framework for Cloud computing services since they usually lack the necessary funds to support advanced and updated data storage and security services.

Neelie Kroes, vice-president of the European Commission responsible for the Digital Agenda, has said "I want to make Europe not just cloud-friendly, but cloud-active. We can deliver cloud computing by using research and innovation to bring about better clouds. Along the way we can modernz our computing infrastructure and give our SMEs a new platform for innovation".<sup>33</sup>

We should bear in mind that balancing citizen's rights and small and medium enterprises interests is the way to ensure the economic and social progress and that the fundamental rights of individuals are safeguarded.

---

33. Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/50>, Towards a European Cloud Computing Strategy World Economic Forum Davos, 27 January 2011.

# **Patenting human genes in Europe: is it possible to set an ethical minimum based on common values?**

---

---

**Leandros Lefakis**

---

---

## **1. Introduction**

The short definition of the gene is that it is a functional unit of the genome. In other words, a gene is a unit of heredity in a living organism. It is a name given to some stretches of DNA (Deoxyribonucleic acid) and RNA (Ribonucleic acid) that code for a type of protein or for an RNA chain that has a function in the organism. It is estimated that there are between 20,000 and 25,000 human protein-coding genes, although it must be pointed out that the estimate of the number of human genes has been repeatedly revised as genome sequence quality and gene finding methods have improved. Earlier predictions estimated that human cells consisted of as many as 2,000,000 genes.

Patenting human genes is generally perceived as ethically controversial. The ethical scruples partly stem from the question of whether it is at all acceptable to patent human genes and partly from the consequences such patenting can have for diagnosis, treatment of illness and disease and research. The most significant question is whether a common understanding on ethical issues can be reached. As a matter of fact, the need to consider moral concerns is pressing in the European patent law. Indeed, the patent law, contrary to other laws, traditionally excludes from patentability inventions which would be contrary to “public order or morality”. These two matters of exclusion are mentioned in the existing law, as well as in Article 53 (a) of the European Patent Convention and the national laws of members - states. Any proposal forwarded should take into account this moral concern, which aims to adapt to the specific case human gene patents which, as based on elements of human origin, involve the issue of fundamental human rights.

This paper wishes to contribute to the general discussion about the ethical defensibility of taking out patents on human genes. Additionally, it wishes to propose some recommendations to the rules in force and to the current practice of granting human gene patents regarding best practices to safeguard ethical considerations in the process.

## 2. Patenting human genes in Europe

### 2.1 *EU regulations*

The legal basis for granting patents at the European Patent Office (EPO) for inventions concerning living organisms, stem-cells and DNA has three elements. The first is the European Patent Convention (EPC), which sets out the general legal principles for granting patents in all technical fields. In addition, biotechnology is to date the only field to have its own special provisions. These are derived from the European Union Directive 98/44/EC on the legal protection of biotechnological inventions, enacted in 1998 by vote of the European Parliament following a ten – year debate between all interested parties. Finally, the national patent laws of each European Union (EU) member - state govern European patents after grant.

The EU “Biotechnology Directive” (98/44/EC) aims to harmonize and define how inventions in the field of biotechnology are to be patented. It affirms that living organisms, cells and gene sequences are patentable and enhances the ethical aspects to be considered when granting patents for biotechnological inventions. The EPO implemented the relevant provisions of the EU Directive into the EPC in 1999. However, a legal challenge against the directive commenced, but finally was rejected by the European Court of Justice in 2001. The Court found that the Directive had been correctly put in place and that it contained sufficient ethical limitations to the patentability of biotechnology. To date, the Directive has been implemented in national laws by the majority of the EU’s member states, including Greece. However, patenting biotechnology remains controversial in respect of the evaluation of important ethical principles such as the respect of human dignity, the adequate protection of the human embryo, the prohibition of financial profit from the human body and body parts, as well as the respect of individual autonomy and the protection of public health. The main problem in applying these principles is that it is often difficult to detect their influence on the patent system. For example, how is human dignity related to patent system? The basic objection to patents on human genes is that they may threaten the individual autonomy, the fundamental principle that everyone should be master of himself, and, in particular of our own bodies, so that one person cannot legitimately acquire control over another person’s body or some part of it. The thought behind this claim is often phrased in terms of “human dignity”. Human dignity is our inherent status as embodied humans. That implies that control over one person’s body cannot be lawfully exercised by another person. Therefore, the important issue is whether individual autonomy really does conflict with patents involving human genes.

## 2.2 The EPO and the EU Directive practice

Like other patent offices, the EPO has been granting patents in the fields of genes for some time. It first granted a patent for a human gene, namely that encoding alpha-interferon, in 1984, and granted another patent for the DNA encoding erythropoietin in 1990. The EU Directive confirmed this long – standing practice by stating in Article 5 that while neither the human body in its natural state nor the mere discovery of one of its elements is patentable, an isolated human element, including a gene sequence, may be patentable, even if it is identical to the natural elements. These two sentences are often regarded as contradictory and merely a creatively worded ploy to enable patents to be granted. Certainly, the underlying purpose is the desire to enable the grant of patents to encourage research in the exciting and promising field of biotechnology. Without patents biotechnology companies have little incentive to make the heavy investment in research and clinical trials required to bring a product in market.

## 2.3 The current practice

It may come as a surprise that patents for genes and gene sequences are today still the subject of such a huge controversy. Patents for so-called “first generation DNA”, i.e. DNA which has been discovered and for which a function has been detected, almost belong to the past. At some point, all genes of interest have been subject to this type of “right investing activity”. It is also surprising to see scientists, organizations or ethical groups persisting in the discussion that patents should not be granted for genes or gene sequences, since they are discoveries and not inventions. Irrespective of the fact that such reasoning is based on an incorrect understanding of the principles of patent law, it is also an argument which has lost *momentum* in all respect. The relevant patents sought now are patents for new applications and functions. Discovering these new functions and applications can hardly be considered not to be patentable subject – matter. But it should be clear that in the case of present day patents for genes related inventions, emphasis should be placed more on the scope of protection of the inventions claimed, than on the very issue of patentability.

## 3. Discovery or invention?

A discovery has to do with any material or phenomenon that exists in nature, including the chemical properties of materials. To be an invention a discovery must also include an intervention that makes use of the material or its properties in a novel way and so provides some new process or product. Discovering a pre-existing aspect of the natural world is not an invention, but applying some innovative step to that new discovery may be. One of the original principles for pat-

ents is that “discoveries” of items that already exist in nature cannot be patented, for these previously existed (“products of nature theory”) and are the common property of all (Bottis 2004). It was stated that the patenting of a gene found in nature is similar to claiming copyright and performance royalties for the song of a bird transcribed into standard musical notation. It was also stated that gene sequences, and the amino - acid sequences in the proteins encoded by nucleic acids, are obviously not inventions if that sequence is found in nature.

The distinction between discovery and invention lies in that a patentable invention has always a practical and technical character, in contrast to a discovery. For example, a natural substance –such as an antibiotic- which has presumably existed for a long time is a discovery in patent terms. However, it could be considered novel if it had not been available to the public before the filing of a patent application. Subject - matter which was previously hidden is not regarded as having been available. Similarly, a human element, such as a gene or a gene sequence, isolated from its natural surroundings is regarded as novel, since it was not available in that form previously. An isolated gene lacks its surrounding DNA, which may influence the expression of the gene. In any case, the novelty of the gene sequences for which patents are filed is a rule beyond doubt, since what is isolated is, in the vast majority of cases, not a gene found in the body, but rather a copy DNA (cDNA) which does not exist in nature. As reflected by the wording of Article 5 of the EU directive, an isolated human element neither is nor regarded as a discovery, since its isolation involves a technical process that adds value to what was known beforehand.

The European Group of Ethics in opinion No 8 on the “Ethical Aspects of Patenting Inventions Involving Elements of Human Origin” stated that the traditional distinction between discovery (not patentable) and invention (patentable) involves, in the field of biotechnology, a particular ethical dimension. What follows from this distinction is that knowledge related to the human body or its elements is relevant to scientific discovery and cannot be patented. It has to be clearly specified that the simple knowledge of the complete or partial structure of a gene cannot be patented.

When patent authorities award patents on genes and gene sequences, it is done on the basis of the criteria of novelty and inventive step. That is to say that the patentholder must in some way have invested some effort to warrant the description of the genuine invention. However, that effort should be confined to creating, with the aid of synthesizing techniques, an artificial molecule in such a way that it contains the same genetic information as the natural gene. However, technological developments have made it possible to map DNA sequences as a matter of routine. As previously, mentioned, however, it is not sufficient to cre-

ate a synthetic copy to obtain a patent on a gene. The applicant must also be able to substantiate that the gene sequence can be used industrially in a way that the gene sequence can be used industrially in a way that has novelty value. Therefore, the patent system rests on the assumption that the patented item constitutes an invention, although some will refute the view that human genes could constitute inventions.

The assertion that patents on genes are patents on discoveries, however, is further complicated by the fact that human genetic material can be modified. For instance, when manufacturing a synthetic gene, a researcher can modify it, so that it is no longer identical with the naturally occurring gene. According to some parties it is arguable whether such a modified gene is an invention or discovery. Our opinion is that it is not even debatable to describe a synthetic gene as a discovery, due to the fact that it has been substantially changed in comparison to the occurring gene.

## **4. What is being patented?**

### **4.1 General issues**

It is often contended that genes should not be patented, since this practice leads to commercialization of the human body. However, patenting cannot be equated with commercialization – many not patented products are sold. The sale of all medicaments is tightly controlled by regulation. Furthermore, the commercialization of elements of the human body is generally accepted and indeed desirable to a certain extent (i.e. insulin, human growth hormone and blood proteins). Moreover, it is often considered inappropriate to grant absolute product protection for a gene or a DNA. Since the number of genes is limited, many genes may be multifunctional. It is feared that research may be hindered by granting protection for all functions and uses. However, this argument applies equally well to all organic chemicals. Not only genes but also many pharmaceutically active molecules possess several often widely different activities. A well-known example is aspirin, which was initially used as a pain – killer but much later was found to help prevent heart attacks as well. This situation is so commonplace that a specially – worded type of patent claim was developed to enable these further medical uses of known products to be patented. The owners of these patents may be dependent on the proprietor of the broad patent and will thus have to obtain a license from the latter in order to practice their inventions. Pharmaceutical companies usually come to cross - licensing agreement, so that a market is seldom blocked by a dominant patent.

As far as DNA is concerned, the argument that DNA should not be patented, as it is a product existing in nature (and is as such a discovery and not an invention)

is not entirely convincing. It is based on a reasoning which does not take into account all “intricacies” of the technology and the patent system. First of all, when a gene or a gene sequence is patented, it is not just merely a matter of patenting a “product of nature”. There is isolation and in some way also purification, as the coding parts of the DNA (exons) are separated from the non-coding parts (introns). It was a very complicated technological task to arrive at such scientific result. Secondly, in most cases it is not the DNA as such which is patented but a cDNA which does not exist in nature, but is synthesized.

#### ***4.2 Actual genes and synthetic copies***

In legal terms, the thing on which a patent is taken out is not the naturally occurring gene, but a synthetic copy, which may nevertheless be “identical to that of a natural element”. From a legal point of view, this is an important point but the question is whether it is also important seen from an ethical viewpoint. Another important issue to be noted is that gene patents deal with the information that can be extracted from working with the genes. For this reason the question of who owns the individual human being’s concrete genes can, according to a number of debaters, be dismissed as impertinent question.

Since the issuance of a patent that deals with human genetic material, a lot of groups and organizations have become fond of asking the question of who “owns” a person’s genes. However, this is not the right question. A more appropriate question would be who owns the intellectual property associated with human genes? Newly discovered genetic material can be patented as long as it is isolated from its natural environment and purified, so as to separate it from extraneous material. In other words, the existence of a patent issued by the EPO owned by companies as “Myriad Genetics” or “Amgen” on purified genes does not mean that these companies own human genes derived from a human body. These human genes are neither “purified” nor “isolated”. Consequently, these companies’ patents do not cover human genes *per se* and that settles any relevant ethical concern.

#### ***4.3 Patenting practice for genes***

Biotechnology patenting practice for genes derives from that applied to other organic chemicals, in particular small molecules such as pharmaceuticals. The isolation of small organic molecules is in itself seldom inventive. What makes a chemical inventive is its non – obvious activity. If inventive step is acknowledged, a patent for the product is given. By analogy to the above, the isolation of genes is nowadays a routine and seldom requires inventive skill. However, if a surprising or unexpected activity or function of the gene (or the protein it encodes) is disclosed by the inventor, the gene is held to be inventive and may be patented.

While additional data supporting the claimed activity may be provided later on, the function must be disclosed initially in the application as filed. Any kind of function is acceptable; it may be of medical use (of the encoded protein), of medical use as a drug target or it may be useful for the diagnosis of a disease. A gene or a gene sequence for which no specific function is described is not regarded as inventive and will not be patented.

It is of significant importance to note that at present filing patents for DNA with only primary functions (i.e. that it codes for a protein) almost belongs to the past, for the simple reason that most genes of interest have already been subject to patent applications. Current and future applications will focus on further applications: genes can be claimed as diagnostic tools, DNA coding for specific proteins, whereby a recombinant vector is produced containing DNA with a specific sequence, genes which control biological pathways, such as in receptors which can then be useful in drug discovery and development, DNA as a promoter, enhancer, polymorphisms, expressed sequence tags (EST's).

## 5. The BRCA genes

BRCA is a human tumor suppressor gene that produces a protein called breast cancer type 1 and type 2 susceptibility protein. It originally constituted for the University of Berkeley at California, as primary evidence for the existence of the gene was provided by the King laboratory at UC Berkeley in 1990. Both genes were later cloned by scientists at "Myriad Genetics". In the United States, methods to isolate and detect BRCA1 and BRCA2 were granted a patent by the United States Patent and Trademark Office (USPTO). On March 29, 2010, a coalition led by the American Civil Liberties Union successfully challenged the basis of Myriad's patents in New York District Court. Patents have been invalidated, but the decision is being appealed.

In Europe Article 53(a) was invoked by several parties who opposed the patent "for methods of diagnosing a predisposition to breast cancer by screening for mutations in the BRCA 1 gene". The main reason for the controversy surrounding this patent is the alleged overcharging of the patent proprietor and whose refusal to grant licences under the patent to third parties wishing to perform tests. The patent was revoked in 2003 for technical reasons, in particular for lack of "inventive step". However, the Opposition Division rejected the objection under Article 53(a) against the patent. The above division referred to a decision (G 1/98) of the EPO's Enlarged Board of Appeal (the highest instance of the EPO), which held that the EPO had not been vested with the task of considering the economic effects of a patent and limiting the claims accordingly. The sole criterion for ob-



jecting under Article 53(a) was whether the exploitation of the invention was contrary to ethics or not.

The BRCA patents, in particular, shook the scientific community. In these patents, a plethora of tests were claimed, all to determine whether a patent had a specific mutation in a gene, which might cause breast cancer in the future. Besides the fact that the patents had very broad claims, there was another reason why these patents caused the turmoil they did. The patent holder ("Myriad Genetics") had decided to pursue a rather aggressive licensing strategy relating to these patents. Myriad granted only exclusive licences, implying that only a very limited number of licensees over the world were allowed to use the technology in the patent and to perform these tests. Such an exclusive licensing system had another adverse effect, a rise in on price, made it rather expensive for research institutions to carry out these tests or to pay the licensee the fee to carry out these tests. In addition, Myriad did not allow local screening, but required the samples be sent to the US.

## 6. Ethical issues

### 6.1 *Guiding principle*

The guiding principle regarding the ethics of patenting DNA is whether the level of protection that is being awarded to inventors by granting gene patents is commensurate -within reason- with the contribution that they have made. In general, patents are defensible and the patent system has to work towards the people's benefit. However, two questions have to be answered. Do patents for these human genes meet the legal criteria? And, is the overall effect of allowing these uses to be claimed in patents beneficial in terms of public interest?

We believe that, as a point of departure, an overall ethical evaluation of the patent system in respect of gene patents is needed. In patent law emphasis has to be laid on the distinction between the original genes and the synthetic copies of the genes. This distinction is hardly of great importance regarding the ethical evaluation of the patent system. An essential aspect of the genes is their content of information, being common to mankind for the most part, and at the same time containing a small part that is unique to every individual. This information content is identical in naturally occurring genes and synthetic copies, thus giving rise to ethical concerns. For example, a broad patent claim on particular genes (whether it is the original gene or a synthetic copy) can prevent scientists -other than the patentholder- from carrying out diagnostic examinations on the gene under consideration. Accordingly, the practical consequences are the same.

Another important distinction in patent law lies between discovery and invention. It is true that in genetics many so-called inventions are actually speaking

discoveries and that the current practice of granting patents to these discoveries is dubious. So, it might be seen as a violation of common morality that private interests can secure rights over phenomena or processes that were discovered by nature long before mankind was capable of identifying them. Man's genetic material should be regarded as a common property as it contains information which is common to mankind. Therefore, everyone should have a share in that knowledge and the therapeutic options developed on the basis that should be available for everyone, which also implies that it could not be blocked by broad patents. Moreover, it is widely supported that health services should not be allocated purely on the basis of financial resources.

The special *status* of genes as carriers of information about the individual as well as all living beings does mean that patenting needs to be done with greater consideration for both the individual and the common good than when patenting traditional materials. The possible advantages of patenting genes, particularly the development of new knowledge and new therapeutic opportunities, must be weighed up against the undesirable consequences of the commercialization and, especially, the monopolization of diagnostic and therapeutic options and the risk of research environments becoming more exclusive.

## **6.2 Recommendations**

On the condition that human gene patents will continue to be granted in the future all legal criteria should be met (new, novel, industrial applicability). Moreover, a number of more specific recommendations concerning the regulation of the patent field should be made. Specifically:

- It should not be possible to award broad gene patents where the patentholder is given sole rights over several possible applications of a particular gene as this may have a negative effect on the development of new treatment and diagnoses. Only narrow patent claims with a precise, detailed description should be issued. Broad patents can have an outright inhibiting effect on the development of new treatments and diagnoses. In addition, the benefit which the intended use is expected to provide must also be specified to ensure that only new inventions of substantial general beneficial value could result in a patent.

- More emphasis should be given to granting compulsory licences in order to prevent anyone from enforcing its patent in a way that unreasonably prevents others from developing new diagnoses and therapies. A compulsory licence can be considered if a company enforces its patent in a way that unreasonably prevents others from developing new diagnoses and therapies. It must be pointed out that the possibility of a compulsory licence is rarely exploited, but this route has to be

taken more often in cases where enforcement of a patent is at odds with the interest of the public interest.

- The patent rules should be formulated so as not to prevent research. Furthermore, researchers should not be under an obligation to patent results in the area of basic research. People whose genes are used in research that leads to applications for patents should give their written consent to the research activities and this should also include consent to the possible result of the research activity being patented.

- The present rules on human gene patents are both very obscure and complex, which creates both a fairness issue and a practical problem. It has been suggested that a possible tool which would eliminate these problems would be to set up independent bodies (both at national and European level) to undertake an ethical and legal evaluation of specific patent applications relating to genes and gene sequences.

- Other means outside the patent system, such as price regulation, could also be instrumental in counteracting the possibly “deleterious effects” of broad patents for science and the right of freedom of research.

- Significant ethical principles such as respect of human dignity and individual autonomy, the prohibition of financial profit from the human body, the protection of public health should be the landmarks for any issue regarding patents that deal human genes or cells.

- The collection or sampling of elements from a human being relies on the consent, cooperation and generosity of the person collaborating in the research. This collection or sampling may raise ethical concerns regarding the information provided to the donor, his consent concerning the future use of the elements, whether it is used for research or commercial purposes, and the compensation he may claim.

- The ethical principle of informed and free consent of the person, from whom retrievals are performed, must be respected. This principle includes that the person in question should be completely and specifically informed, in particular on the potential patent application of the invention which could be made from the use of this element. Any invention based on the use of elements of human origin, which have been retrieved without respecting the principle of consent will not fulfill the ethical requirements.

### **6.3 In search of “common values”**

It is not a *utopia* to commence a discussion on whether the values stated in international conventions should serve as an expression of common and shared

values on a European level. European governments have signed the 1950 European Convention on Human Rights, the Council of Europe's 1997 Convention on Human Rights and Biomedicine, the European Charter of Fundamental Rights and UNESCO's 1997 Universal Declaration on the Human Genome and Human Rights. The problem in applying these values is that it is often difficult to detect their influence on the patent system. For example, how is human dignity related to the patent system? Moreover, in many cases these values and rights have to be balanced against each other and this is, for instance, highlighted in Article 2 of the Council of Europe's Convention on Human Rights and Biomedicine, according to which "the interest and welfare of the individual shall prevail over the sole interest of society and science".

It is suggested that all common values could be redefined by means of social research. However, a much more pragmatic view should be heard by examining an unresolved conflict between ethical philosophy or research and certain impatience with theorizing. Religious and cultural frameworks vary very widely across Europe. If we try to establish a "common value system", it has to be based on a scientific understanding of human life. This means not to look for some abstract ethical concepts and theories, but at practical questions in respect of issues such as scientific progress, health or human suffering.

The reality is that EPO has to grant patents and ethics is part of the evaluation. Therefore, a kind of common notion on how we interpret ethics has to be reached. However, the main issue is that even if we could agree on some ethical values or approaches, how could we incorporate them in the patent system? European patent law framework already incorporates ethical concerns, but it is a matter of assessment to examine whether further regulation is needed. The idea of an independent body to perform ethical evaluation has been proposed, as a practical solution to all the above issues. We believe that Europe may not be large enough for a full debate and overview of the ethics of patenting human genes. We are obliged to discuss about the reality on a global level. Without a global discussion about ethical patenting it would be very difficult to establish a rational legal framework regarding the enforcement of these patents.

## 7. Conclusion

It is true that patents had been granted on genes according to the rules of the existing patent system, before scientists acquired an in-depth knowledge of the function of human genes. Moreover, no one could deny that genes differ from the traditional materials for which the patent rules were designed. This is the reason why we believe that it is time to re-embark on a thorough ethical discussion of the problems and advantages of permitting patents on human DNA.

Even though values set in international conventions and charters could be seen as an expression of shared European values, the content of these values may vary among countries and cultures. However, it might be possible to detect shared European values, e.g. by way of surveys into how people actually feel about which values should be used to regulate different sorts of technology. Additionally, a more case - oriented approach might be a good way to identify possible common values at European level. Even if it might not be possible to distinguish important common values, such as informed consent or human dignity, it could be achievable to identify values of a more procedural kind, such as transparency, honesty and willingness to respect different points of view. Finally, as for the question of how the common values -given that they can be established- can be incorporated in the patent system, it is suggested that on a national level ethical concerns should be incorporated in the general rules of the patent system. On a EU level it would be a huge step forward if an ethical advisory board were set up to perform ethical evaluations of specific patent applications for the EPO. Concerning the inventions deriving from the knowledge of a human gene or a partial human gene sequence, the granting of a patent is acceptable only if the identification of the function attached to a human gene, or a partial human gene sequence allows new possibilities (for instance the production of new drugs), on the one hand and, on the other hand, if the intended use of the patent is sufficiently specified and identified. The complexity and sensitivity of the issues raised by patenting in the field of human gene patents require us to make every effort to inform citizens of the technical, scientific and social as well as ethical aspects of those issues. The affirmation of the citizens' rights in the EU implies that the economical advantages derived from biotechnological developments should in no way affect the respect of ethics.

## References

Bostyn S.J.R., DNA Patents in Europe: Controversy Remains, in "Patenting Human Genes and Stem Cells – A Report", The Danish Council of Ethics, 2004, 27.

Bottis M., Information Law, Nomiki Vivliothiki, 2004 (in Greek).

Commission of the European Communities, Report from the Commission to the European Parliament and the Council on the Development and Implications of Patent Law in the Field of Biotechnology and Genetic Engineering, Brussels 7.10.2002, COM (2002) 545 final.

Cornish W.R., Intellectual Property. Patents, Copyright, Trade Marks and Allied Rights, 3rd edition, Sweet & Maxwell, London, 1996.

Council of Europe, International Conference of the Council of Europe on Ethical Issues Arising from the Application of Biotechnology, Oviedo, Spain, May 1999.

Eisenberg R.S., Patenting the Human Genome, (1990) vol. 39, Emory Law Journal, 722.

European Commission, The European Group on Ethics in Science and New Technologies (EGE), Bruxelles, 1998.

European Group on Ethics in Science and New Technologies, Opinion no. 4 on the Ethical Implications of Gene Therapy, 13 December 1994.

European Group on Ethics in Science and New Technologies, Opinion no. 8 on the Ethical Aspects of Patenting Inventions Involving Elements of Human Origin, 25 September 1996.

Galloux J.C., Essai de définition d'un statut juridique pour le matériel génétique, Thèse, Bordeaux, 1988.

Galloux, J.C., Première vue sur la directive relative à la protection juridique des inventions biotechnologiques, La semaine juridique, 21 Octobre, 1998.

Gannon P., Guthrie T., Laurie G.T., Patents, Morality and DNA: Should Be Intellectual Property Protections of the Human Genome Project?, (1995) vol. 1 Medical Law International, 321.

Lefakis L.K., Biotechnology Patents, Sakkoulas Publications, Athens – Thessaloniki, 2003 (in Greek).

Lefakis L.K., Human gene as patentable subject-matter, (2006) Commercial Law Review, 1113 (in Greek).

Looney B., Should Genes Be Patented? The Genes Patenting Controversy: Legal Ethical and Policy Foundations of an International Agreement, (1994) vol. 26 Law and Policy in International Business, 231.

Moufang R., Patenting of Human Genes, Cells and Parts of the Body? - The Ethical Dimensions of Patent Law, (1994) vol. 25 no. 4 IIC, 487.

Roberts C., The Prospects of Success of the National Institute of Health's Human Genome Application, (1994) 1 EIPR, 30.

Scalise D., Nugent D., Patenting Living Matter in the European Community: Diriment of the Draft Directive, (1992-1993) vol. 16 Fordham International Law Journal, 990.

Schatz U., Patentability of Genetic Engineering Inventions in the EPO Practice, [1998] 1 IIC, 2.

Sterckx S., European Patent Law and Biotechnological Inventions, in Sterckx S. (ed.), *Biotechnology Patents and Morality*, 2nd edition, Ashgate, Publications, Aldershot, 2000.

Straus J., *Industrial Property Protection of Biotechnological Inventions. Analysis of Certain Basic Issues*, WIPO, 1985.

Van Overwalle G., *Study on the Patenting of Inventions Related to Human Stem Cell Research*, European Group of Ethics and New Technologies to the European Commission, European Commission, Luxembourg, 2002.

Varbeure B., Matthijs G., Van Overwalle G., *Analysing DNA Patents in Relation with Diagnostic Genetic Testing*, [2006] *European Journal of Human Genetics*, 14.

Vogel F., Grunwald R. (ed.), *Patenting of Genes and Living Organisms*, Springer Verlag, Berlin – Haidelberg, 1994.

Thomas S., *The Ethics of Patenting DNA*, in “*Patenting Human Genes and Stem Cells – A Report*”, The Danish Council of Ethics, 2004, 113.

# Rejecting the works of Dan Flavin and Bill Viola: revisiting the boundaries of copyright protection for post-modern art

---

---

Marina Markellou

---

---

Visual arts have expanded from their traditional territories of painting, drawing, printing and sculpture to embrace new techniques, methods and to produce installations, interactive artworks on an ever larger and more spectacular scale and in mixed media and environments<sup>1</sup>. In overall there has been considerable confusion about the definition of an artwork and its protection for copyright purposes susceptible of other benefits such as tax exemption or reduction. When judges struggle with the meaning of the words and expressions like “artistic” and “artistic quality”, when they lay down arbitrary rules about what constitutes an artistic work, when they struggle with the idea/expression dichotomy, what they may be demonstrating is a particular discomfort with the nature of creativity in the visual arts<sup>2</sup>.

This paper discusses one exceptional trial that has addressed the question “what is sculpture?”: *Haunch of Venison and Partners v. Her Majesty’s Revenue & Customs*<sup>3</sup>. The case raises questions about the correct classification of video installations for the purposes of the Combined Nomenclature in Council Regulation 2658/87/EEC. Under the relevant E.C. Customs Tariff, the so-called “Combined Nomenclature”, “sculptures” imported into the EC are charged a reduced rate of 5% and are not liable for customs duties which apply also to the U.K. It is important to observe that under the “Combined Nomenclature” there is no explicit category of protection for “artworks”, rather artworks are classified in terms of their medium, e.g. the heading number 9703 “original sculptures and statuary, in any material”. Therefore there is no explicit category for installations or video installations. Nevertheless, Chapter Notes 4 of the so-called “Combined Nomenclature” requires that where there is doubt about a classification of a work that is in fact

- 
1. Petry M., *The Art of not making; the new artist/artisan relationship* (London: Thames &Hudson 2011), 11.
  2. Macmillan F., «Is copyright blind to the visual?», (2008) 7 *Visual Communication* 110, 97-118.
  3. *Haunch of Venison Partners Limited v. Her Majesty’s Commissioners of Revenue and Customs*, London Tribunal Centre, released on 11 December 2008 and is available at: <[http://www.tax-bar.com/Haunch\\_of\\_Venison\\_Trib.pdf](http://www.tax-bar.com/Haunch_of_Venison_Trib.pdf)>.



a work of art, preference should be given to one of the Chapter 97 headings over those of any other Chapter.

The British Customs Authorities sought payment of approximately £36,000 customs duty on six works by the American artist Bill Viola, on their importation into the UK, as being properly classifiable as “image projectors” and on a work, by the deceased American artist Dan Flavin, as being classifiable as “chandeliers and other electrical ceiling or wall lighting fittings”. Haunch of Venison Partners Limited, a commercial gallery specialising in modern and contemporary works, appeals before the VAT British Tribunal. The gallery claims that the goods in question should be classified as “original sculptures and statuary, in any material” or alternatively as “collectors’ pieces of historical interest”. The economical aspect of this appeal is to avoid paying the full VAT rate for importations instead of the one of 5% VAT that corresponds to the works of art.

At the Tribunal’s hearing, Haunch of Venison argued that a sculpture should be understood to refer to “all three dimensional artistic productions, irrespective of the techniques and materials used”. Therefore, the Viola works are three dimensional. They do not consist of a two dimensional image on a screen. The artist specified exactly what had to be used and how it had to be installed in much the same way as for the Flavin work. On the other side, and in respect of both the Viola works and the Flavin work the respondents assert that, because the works are not imported in one piece but are taken apart for transportation, they should be classified according to the classification of their separate parts. They argued that Viola’s work in question was only the projection emanating from the screen which is itself a flat object and that it is simply incorrect as a matter of fact to consider the mechanism by which that image is realized as being part of a sculpture even if that mechanism does have a three dimensional form. According to them, the works in question are not works of art viewed objectively when they arrive in separate pieces and that if these works as presented to the customs authorities are treated as works of art at that stage then any importer could declare any goods to be works of art and thereby circumvent the positive rates of duty. Her Majesty Revenue and Customs provided no witness evidence to support its claims during the hearing in contrast to Haunch of Venison<sup>4</sup>.

The British Tribunal took into serious consideration the evidence by eminent art experts and decided that the Viola works are sculptures and, as is often the case for sculptures of the most traditional kind, that conclusion is not contradicted by

---

4. See also the analysis of this case by D. McClean who was a member of the legal team representing the appellant at the hearing, in McClean D., “I Would prefer not to”- The Legal Judgment of Art: The Trials of *Brancusi v. United States* (1928) and *Haunch of Venison & Partners v. Her Majesty’s Revenue & Customs* (2008)”, (2011) 38 *Propriétés Intellectuelles*, 20-24.

the fact that the works may have been made in editions of small numbers. Each was individually made by Viola and is an original work even though the DVD may have contained the same digital material for each copy of the edition. The Tribunal regarded “it as absurd to classify any of the works as components ignoring the fact that the components together make a work of art”<sup>5</sup>.

The Tribunal also hold that the Viola works are three dimensional. They do not consist of a two dimensional image on a screen. The artist chose all the components he supplied as part of the work deliberately and as part of the artistic process with a view to achieving his artistic intention with the greatest effect. He did not intend that the works should be shown on just any randomly selected DVD player in just any room or space in which that player happened to be. No issue arises as to whether the Flavin work is three dimensional.

Following the British decision, in August 2010, the European Commission has amended the classification of goods in the Combined Nomenclature to emphasise that goods upon importation should be classified in terms of their constituent parts. In order to ensure uniform application of the Combined Nomenclature annexed to Regulation (EEC) no 2658/87, the European Commission adopted the Regulation (EU) No 731/2010 of 11 August 2010 concerning the classification of certain goods in the Combined Nomenclature<sup>6</sup>.

The European Commission clarified that video-sound installations (as Viola’s works) and light installations (as Dan Flavin work) should be classified accordingly to the general rules with the full VAT rate. Concerning the video-sound installations consisting essentially of components such as video reproducing apparatus, projectors, single self-powered loudspeakers and DVD’s containing recorded works of “modern art” in the form of images accompanied by sound, classification as sculptures is excluded. None of the individual components or the whole installation, even when assembled, can be considered as a sculpture. The components have been slightly modified by the artist, but these modifications do not alter their preliminary function of goods. It is the content recorded on the DVD which, together with the components of the installation, provides for the ‘modern art’.

As for the Dan Flavin’s work the Commission stated as follows: “Classification as a sculpture is excluded, as it is not the installation that constitutes a ‘work of art’ but the result of the operations (the light effect) carried out by it”.

---

5. Paragraph 49 of the Tribunal’s Decision.

6. Commission Regulation (EU) No 731/2010 of 11 August 2010 concerning the classification of certain goods in the Combined Nomenclature, *JO* L214/2, 14-8-2010.

Why did the European Commission go to such elaborate lengths to overturn the decision of a London VAT Tribunal in relation to a relatively small amount of import tax in relation to artworks? In fact 'within weeks of the London Tribunal decision, the issue was on the agenda of the European Commission's Customs Code Committee in Brussels. Several Member States reported that their tax authorities had considered the issue of video art previously. During the meeting it was told that in two Member States (the UK and the Netherlands), a VAT Tribunal had held that video installations should be classified as sculptures. By April 2009, without apparent further public consultation or consultation with relevant members of the art world, the Committee decided that a draft regulation will be prepared for a future meeting. One of the appellants' legal attorneys argued that "the EC's definition of art (in the Regulation) is a patently absurd piece of legislation. Adopted behind closed doors, without an apparent understanding of the subject matter, it reverses two national judicial decisions that both ruled that video installations should be classified as art. No judge had decided the issue in any other way. There was no need for the Regulation, which is contrary to the jurisprudence of the European Court of Justice"<sup>7</sup>.

In line with the appellants' arguments, there are some previous rulings delivered by the European Court of Justice that happen to be in conflict with the Regulation. The *Reinhard Onnasch v. Hauptzollamt Berlin-Packhof* Case (155/84) in which the European Court of Justice held that a work by Claes Oldenberg made mainly from cardboard and polystyrene was a work of sculpture. In fact, the European Court's ruling could be considered as a more expansive interpretation of the classification of artwork provided in Chapter 97 of the "Combined Nomenclature".

There is also the *Krystyna Gmurzynska-Bscher v. Oberfinanzdirektion Köln* Case (C-231/89) in which the work in question was a steel plate with a fused coating of enamel-glaze colours by Lazlo Moholy-Nagy. The European Court of Justice held that where an object is an original work of art that precludes it from being a decoration, it must be classified under Chapter 97.

Both Rulings said that sculpture should be understood to refer to "all three-dimensional artistic productions, irrespective of the techniques and materials used".

It is not the first time that a judge, trained only to the law, is called upon in a court to precisely judge what is Art. In October 1926 United States Customs officials characterized Brancusi's sculpture 'Bird in Space' as "Kitchen Utensils and

---

7. Adam G., "Flavin and Viola light works ruled "not art", *The Art Magazine*, 219, December 2010, available at: <<http://www.theartnewspaper.com/articles/Flavin-and-Viola-light-works-ruled-not-art%E2%80%9D/22069>>.

Hospital Supplies” by classifying it as such. Under the provision of Article 1704 of the US Tariffs Act 1922, works of sculpture were exempt from importation duty, which was otherwise charged 40% on the value of constituent materials. Brancusi formed an appeal against the US customs’ decision that led to the celebrated trial in the Third Division US Customs Court<sup>8</sup>. At stake in the trial was the application of the Article 1704 of The Act. According to the provision, a work of sculpture must be the original production of a professional sculptor. The judge stated that “while some difficulty might be encountered in associating it [the sculpture] with a bird, it is nevertheless pleasing to look at and highly ornamental, and as we hold under the evidence that it is the original production of a professional sculptor and is in fact a piece of sculpture and a work of art according to the authorities above referred to, we sustain the protest and find that it is entitled to free entry”.

In finding in favour of Brancusi, one of the most interesting parts in Justice Waite’s conclusion is the consideration that “in the meanwhile there has been developing a so-called new school of art whose exponents attempt to portray abstract ideas rather than to imitate natural objects. Whether or not we are in sympathy with these newer ideas and the schools which represent them, we think that the fact of their existence and their influence upon the art world as recognized by the courts must be considered”<sup>9</sup>.

Eighty years later it does not seem in the least surprising to find that an abstract artwork could be regarded as a work of sculpture...

## As a conclusion

The growth in the twentieth century of forms of artistic practice focusing on the process rather than just the product, have posed a particular problem for the copyright definition of “artistic works”. A range of contemporary art forms seem to raise problems of characterisation including works such as Gilbert and George’s living sculptures, Kounellis’ *arte povera* works, Yves Klein’s monochrome tables, Marina Abramovic’s performances and many other forms of post-modern art<sup>10</sup>.

8. *Brancusi v. United States* (1928) in M. Rowell, *Brancusi v. United States: The Historic Trial 1928* (Paris: Société Nouvelle Adam Biro, 1999).

9. *Ibid.* p. 115.

10. For a vigorous analysis see Walravens N., *L’oeuvre d’art en droit d’auteur, Forme et originalité des oeuvres d’art contemporaines*, (Paris: Economica 2005). See also the two recent French Decisions regarding two tables of Yves Klein that were considered by the judges as original works of art, protected by the French Copyright law in Walravens N., “Les tables d’Yves Klein, peintre de l’Immatériel, protégées par le droit d’auteur”, (2011) 70 *Propriétés Intellectuelles*, 6-12.

When drawing distinctions between art and other components, it seems that there is an important element that should be taken into consideration by the judges, the creative process. The French judges did not stay insensible and relatively soon they took into account the creative process of wrapping the “Pont-Neuf” bridge by artists Christo and Jeanne Claude. The Court of Appeal of Paris concluded that the idea of highlighting the pureness of the lines of a bridge and its lampposts by means of a cloth and ropes constitutes an original work that merits legal protection<sup>11</sup>. As Professor Treppoz observed, “for the Court of Appeal of Paris, the creative process is not limited purely to the wrapping phase but extends, beforehand, to the choice of the object to be wrapped. The creation is not limited to the composition; it extends to the idea which thus obtains protection. While a banal idea –wrapping objects- is not protected, an original idea –wrapping the Pont-Neuf- may be”<sup>12</sup>. More recently, in *Jacob Gautel v. Bettina Rheims* case the French Court took under consideration the artist’s choices by considering that the combination of different elements demonstrates a certain level of creativity and of sensibility that should be protected by Copyright law<sup>13</sup>.

Concerning Viola’s work, the artist chooses each component and he gives precise instructions about how the work should be shown including the equipment to be used and indeed the equipment is supplied as part of the work when it is sold. The Flavin work can be described by its title: “six alternating cool white/warm white fluorescent lights vertical and centred (1973)”. Flavin works use ordinary lighting components -though of high quality- but the artist specified exactly what had to be used and how it had to be installed in much the same way as for the Viola works. The works are accompanied by detailed instructions drawn up by the artist. The artist also adopted a policy of never supplying a duplicate of the certificates of authenticity, which he supplied when he sold a work, so that authentic copies could not be made.

In overall, the process of creation is akin to other artistic mediums that strive to achieve something unique and inspirational and should be taken into considera-

---

11. Paris Court of Appeal, 13 March 1986, (1987) *Dalloz somm.* 150.

12. Treppoz E., «What legal protection(s) for contemporary art?» (2006) 209 *RIDA*, 51-126.

13. French Supreme Court, 13 November 2008, no 06-19.021, *Bull. Civ. I*, no 258. See some interesting comments about this case in Caron C., “L’ Art conceptuel au paradis de la Cour suprême», (2009) 1 *Communication Commerce Electronique*, 23-24; Gaudrat P., «De l’enfer de l’addiction au paradis des toilettes: tribulations judiciaires au purgatoire du droit d’auteur», (2009) 220 *RIDA*, 81-171; Treppoz E., “La Nouvelle Eve au Paradis du droit d’auteur, suite et fin», (2009) *Dalloz*, 266-268.

tion by Courts<sup>14</sup>. However, this is not an easy task due to the fact that the creative process draws upon the influence of earlier works with the result that overprotection of those works will stifle creativity<sup>15</sup>. In this context, the main tool for achieving the balance between the protection of creativity and the stimulation of further forms of creativity is the need for an extensive approach of creative expression. This would include the arrangement of post-modern artworks inside copyright protection, when the other criteria for copyright purposes are met. The Black Square presented in 1915 by Kazimir Malevich, the monochrome blue by Yves Klein, the Readymades by Marcel Duchamp, all these works of art cannot be reduced into an idea, though, they do illustrate the difficulty in distinguishing the idea from the expression<sup>16</sup>. Under these circumstances, a more extensive view of the form, that will include all the critical phases of creation, from the beginning of the creative process to its result, should be taken into consideration. The form must be understood in a broad sense, encompassing all languages perceptible to the senses. The work must be understood *lato sensu*, embracing the space, the time and interacting with its public.

Another important issue to be raised is that Courts should proceed to a liberal interpretation of legislations in order to be capable of embracing new artistic techniques as it has been established in Onnash case. As the judges stated in Viola and Dan Flavin case, "but legislation cannot be interpreted on the basis that it should be made as easy as possible for the authorities to apply it, even if that means interpreting it in an absurd manner which the respondents' argument invites us to do. We regard it as absurd to classify any of these works as components ignoring the fact that the components together make a work of art". As already noted, "as Courts have done in the past with photography, it seems possible and likely that Courts and Legislators will begin to recognize "art" in its multitudinous formats and will protect it according to the spirit of copyright law"<sup>17</sup>.

Lastly, it seems that another element should be carefully be observed: the perception of the public. Contemporary artistic practice establishes a close intimacy

---

14. See Torsen M.-A., "Beyond oil on canvas: new media and presentation formats challenge international copyright law's ability to protect the interest of the contemporary artist", (2006) 3:1 *SCRIPT*-ed.

15. Boggs J S G, "Who owns this?", (1993) 68 *Chicago-Kent Law Review*, 898-900. See generally, Macmillan Patfield F., "Towards a reconciliation of free speech and copyright" in E Barendt (ed), *The Yearbook of Media and Entertainment Law* 1996 (1996) 199.

16. Masiyakurima P., "The futility of the idea/expression dichotomy in uk Copyright law", (2007) 38 *IIC*, 548-572.

17. Torsen M.-A. "Beyond oil on canvas: new media and presentation formats challenge international copyright law's ability to protect the interest of the contemporary artist", *op.cit.*, p. 70.

with the viewer. The concept of “open work”, imagined by Umberto Eco, finds its concrete expression to the conceptual “art attitudes” and to performances. This openness, this kind of interactivity between art and the public, traditionally rejected by the legal system of copyright, fortunately does not leave indifferent the judge. The public perception of video and light installations as a form of art is evident in the culture surrounding events. The inclusion of this new form of works in museum exhibits should not be underestimated. However copyright’s definition of creative expression is not necessarily coextensive with that of the art community. How judges would be able to perceive these new forms that not only transgress the classic aesthetical rules but they also call for the interactivity of the spectator<sup>18</sup>?

A recent decision that comes from United States concerning the qualification of a living garden installation as a work of art, ruled that Chapman Kelley’s art installation “is neither ‘authored’ nor ‘fixed’ in the senses required for basic copyright”. The district judges worried about taking “too literalist an approach to determining whether a given object qualifies as a sculpture or painting”<sup>19</sup>. The Court considered that “we fully accept that the artistic community might classify Kelley’s garden as a work of postmodern conceptual art. We acknowledge as well that copyright’s prerequisites of authorship and fixation are broadly defined. But the law must have some limits; not all conceptual art may be copyrighted”.

The reluctance of judges to protect under copyright law works that could be characterized as simple manufactured objects or simple combinations of ordinary elements is understandable. It is undeniable that art is moving faster than its legal framework. The frontiers are not easily drawn between the non-protectable ideas and works embodied protection. However, the flexibility of law has proved through centuries its capacity to protect in an efficient way the noblest of creations, even though we should not underestimate Justice Holmes’s warning when stating that “it would be a dangerous undertaking for persons trained only to the law to constitute themselves final judges of the worth of pictorial illustrations, outside of the narrowest and most obvious limits”<sup>20</sup>.

---

18. See the interesting presentation of the French judge A. Girardet during the conference organized in Paris in September 2010 for the 20th anniversary of the Franco British Lawyers’ Society in “Le droit à la recherche de l’artiste”, (2011) 38 *Propriétés Intellectuelles*, 17-19.

19. *Chapman Kelley v. Chicago Park* case, District Decision 16 February 2011.

20. *Bleistein v. Donaldson Lithographing Co.*, 188 U.S. 239, 251 (1903). See also Bottis M., “Information Law, Nomiki Vivliothiki, 2004.

# Audiovisual works as intellectual property

---

---

Maria Markova

---

---

## 1. Introduction

We identify the result of the creative work of an artistic and independent team, including a scriptwriter, a director, an operator and an artist for cartoons as audiovisual work. The products of their activity in the form of scientific, science - fiction, documentary or other form are an intellectual result. As an intellectual result the audiovisual work is an object of intellectual property, in particular as an object of artistic property /copyright as a legal term/.

The term “intellectual property” refers broadly to the creations of the human mind. Intellectual property rights protect the interests of creators by giving them property rights over their creations.

The Convention Establishing the World Intellectual Property Organization (1967) does not seek to define intellectual property, but gives the following list of the matter protected by intellectual property rights:

- literary, artistic and scientific works;
- performances of performing artists, phonograms, and broadcasts;
- inventions in all fields of human endeavour;
- scientific discoveries;
- industrial designs;
- trademarks, service marks, and commercial names and designations;
- protection against unfair competition; and
- “all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields.”

Intellectual property relates to items of information or knowledge, which can be incorporated in tangible objects at the same time in an unlimited number of copies at different locations anywhere in the world. The intellectual property includes two main groups of property: artistic property /copyright as a legal term/ and industrial property /complex of patent, design, indications and competitive law as a wide legal terms.

The importance of protecting intellectual property was first recognized in the



- *Paris Convention for the Protection of Industrial Property* in 1883 and
- the *Berne Convention for the Protection of Literary and Artistic Works* in 1886.

The World Intellectual Property Organization (WIPO) administers both treaties.

The object of protection is the audiovisual work· work, including in itself images, movements and/ or voices. A working definition is that an audiovisual work is a series of interconnected images, fixed on any type of medium, with or without sound, perceived as a moving picture and used in any manner.

The subject – holder of protection is the collective body of writer, director, operator and artist, in the case of cartoons. The other legal name for the subject-holder is an author. In this case it is a collective body of many natural persons–the creators.

Audiovisual work is an object of protection automatically, without any requirements for registration or deposit of the original work or its copies regarding the copyright law. There are no requirements for novelty of the art idea to protect any work. The only requirement is that the artistic work has to be presented in a new original way, in a new original form.

Originality is explained as a term by J. Phillips and A. Firth to their work “Introduction to intellectual property law”, (1990, p. 223-226) as a casual relation between author’s creative conception and the work as a result of his creative work. These are: skillfully, insight, work.

Every work is under protection, independently of its form and art qualities. No need to be presented to the public. The fact of its materialization is enough to arise all of the rights.

Copyright in the field of the audiovisual works (AVW) is under regulation in many normative acts on national, regional and international level. The most important are the Bern Convention for the protection of literature and art works, the Rome convention for the rights of performing artist and producer, the TRIP’s agreement, the WIPO Copyright Treaty and the WIPO performances and Phonograms Treaty. For the purpose of this paper we focus on the Bern Convention and the Bulgarian Copyright Law.

## **2. Main principles of the Bern Convention, 1886**

Bern Convention is the major act in the field of literature, science and artistic works. Its main aim is to protect more effectively moral and economic rights of the creators and their heirs.

Principles of the Bern Convention are:

1. The principle of nationality: authors shall enjoy, in respect of works for which they are protected under this Convention, in countries of the Union other than the country of origin, the rights which their respective laws do now or may hereafter grant to their nationals, as well as the rights specially granted by this Convention.
2. The principle of automaticity: the enjoyment and the exercise of these rights shall not be subject to any formality; such enjoyment and such exercise shall be independent of the existence of protection in the country of origin of the work. Consequently, apart from the provisions of this Convention, the extent of protection, as well as the means of redress afforded to the author to protect his rights, shall be governed exclusively by the laws of the country where protection is claimed.
3. The principle of independence: domestic law governs protection in the country of origin. However, when the author is not a national of the country of origin of the work for which he is protected under this Convention, he shall enjoy in that country the same rights as national authors.

The country of origin shall be considered to be:

- a) in the case of works first published in a country of the Union, that country; in the case of works published simultaneously in several countries of the Union, which grant different terms of protection, the country whose legislation grants the shortest term of protection;
- b) in the case of works published simultaneously in a country outside the Union and in a country of the Union, the latter country;
- c) in the case of unpublished works or of works first published in a country outside the Union, without simultaneous publication in a country of the Union, the country of the Union of which the author is a national, provided that, when these are works of architecture erected in a country of the Union or other artistic works incorporated in a building or other structure located in a country of the Union, the country of origin shall be that country.

### **3. Protection of the audiovisual work according to the Bulgarian copyright law, 1993**

First of all, I would like to emphasize that the Bulgarian copyright law is fully synchronized with the international and European copyright law.

The main standing in the Bulgarian copyright law is:

Object of protection is: any literary, artistic and scientific work resulting from a creative endeavour and expressed by any mode and in any objective form shall be the object of copyright.

In particular the objects of copyright protection as audiovisual works are:

- The result of scientific researches in the form of audiovisual works;
- multimedia presentation;
- other results of the academic work in the way of audiovisual work;
- documentaries;
- films in the categories: science fiction; drama works; comedy works; historical; criminal, fantasy; musical; thriller, horror movie; soap operas, military, mysteries, situation comedy and other kinds;
- cartoons and animation.
- collection of instructions, exercises, methods, lessons, etc., fixed on a CD holder.

Professionals in audiovisual works are discussing such terms as films and other audiovisual materials; “digital work” and “web-design”, “interface design”, “software work”, etc. The main characteristic of those works is the mixture of sound, movement and/ or images.

Subject-holder of the author’s rights on the audiovisual work could be:

- **author of the work**, “an author is a natural person whose creative endeavour has resulted in the creation of a literary, artistic or scientific work. Other natural or legal persons may be copyright proprietors only in the cases provided for under this Act”.
- Until proved otherwise, the person whose name or other identifying mark is inscribed in the customary manner on the literary, artistic or scientific work, shall be considered its author.

Copyright over works created by two or more persons shall belong to them jointly irrespective of whether the said works constitute one indivisible entity or consist of separate parts each having individual significance. In this case we are identifying this work as a joint authorship.

Copyright over audiovisual works belongs to the persons that form the collective body of the author:

- the director,
- the author of the screenplay,
- the director of photography

and

- the artist director in cartoons.

The author of the music, the dialogue, the pre-existing literary work on which the AVW are based, the costume designers and the authors of all other material, incorporated in the AVW, shall enjoy the copyright in their individual works.

#### **4. Exclusive rights on the audiovisual works**

Copyright on the audiovisual works comes into force at the moment of its creation. Regarding the Bulgarian copyright law the exclusive rights on the audiovisual works origin for its creator or for collective body of the creators.

##### **4.1 *Non-Economic rights /Moral rights***

The author shall be entitled to:

- decide whether a work created by him may be made available to the public and to determine the time, place and manner in which this may be done;
- claim the copyright over such works;
- decide whether such works shall be made available to the public anonymously or pseudonymously;
- require that his name, pseudonym or other identifying mark be identified in a suitable manner whenever his work is used;
- require that the entirety of his work is preserved and oppose any changes therein as well as any other actions that may violate his legitimate interests or personal dignity;
- make alterations in the work inasmuch as this does not prejudice rights acquired by other persons;
- have access to the original of the work when it is in the possession of another person and whenever such access is necessary for exercising non-economic or economic rights;
- halt the use of the work due to changes in his beliefs, with the exception of already implemented architectural works, providing compensation for the damages incurred by persons who have lawfully obtained the right to use the work.

##### **4.2 *Economic rights***

The author shall be entitled to the exclusive right to use the AVW created by him and to permit its use by other persons except in the cases when this Act provides

otherwise. Actions such as the ones listed below shall be considered as ways of use within the meaning of paragraph 1:

- reproduction of the work;
- distribution of the original of the work or copies thereof among an unlimited number of persons;
- public presentation of the work;
- public display of a work of art or a work created by photographic or similar means;
- revision of the work, in order to use the work to create a new derivative work;
- import and export of the work in trade quantities

The author possesses the right to receive a reward for every kind of using of his work and for every consecutive using of such kind.

## **5. Free use of the audiovisual works**

Out of author's exclusive rights on his creative work is the so called "**free use**".

We should define the legal person "user". Regarding the CR law the user can be: physical or legal persons, such as "publishers, theaters, concert organizers, radio and TV organizations, public catering and entertainment establishments, producers of phonograms, film producers, Internet content providers and other, who bring the work to the attention of readers, spectators and listeners directly or through the intermediary of the other persons - distributors".

Bulgarian copyright law defines different forms of free use: permissible use and personal use; free use with compensation or free use with no compensation.

### **5.1 Permissible free use**

No permission by the author and no compensation shall be due in the case of:

- The use of parts of published works or of a moderate number of small works in other works in such a volume as is necessary for the purposes of an analysis, commentary or another kind of scientific research. Such use shall be permissible only for scientific and educational purposes, shall include reference to the source and name of the author, and only when it does not prejudice the normal use of the work and does not result in unjustified damage to the legitimate interests of the authors;

- Reproduction by photographic, cinematographic or similar manner, as well as audio or video recordings of works related to a current event for the use of such works by the media in a limited volume for the purpose of providing news coverage;
- Reproduction of works that are on permanent display on streets, squares and other public places without their being subjected to mechanical contact copying, as well as their broadcasting by wireless means, by cable or other technical means, if this is done for the purpose of providing information or for other non-commercial purposes;
- The public performance of published works in educational institutions if this does not involve the collection of revenues from such performance and if the participants in the preparatory work and the actual public performance do not receive compensation;
- Reproduction by copier or other similar means of parts of published works or of small works by educational institutions and their use for educational purposes;
- Reproduction in small quantities of already published works, with the exception of computer software and data bases, by using copier, photographic or other means by public libraries, document centers, research institutions, etc., if this is done for scientific purposes or to preserve the works and if the copies are not circulated outside the framework of the organization which has made them;

## ***5.2 Free copying for personal use***

- The copying of already published works shall be made without the consent of the author and without compensation only if it is done for personal use. This shall not be valid for computer software and architectural designs.
- The compensation payments shall be made to a designated by the ministry responsible for culture organization, which shall then distribute them among the organizations representing the individual categories of copyright proprietors. Prior to any such distribution, twenty per cent of all sums collected shall be turned over to the ministry responsible for culture to be used for the purposes of culture.
- The distribution of the sums thus collected among the various categories of copyright proprietors shall be made on the grounds of an agreement between the organizations carrying out the collective management of the individual kinds of copyrights.

Nowdays in the digital age and Internet we should pay a special attention to the question of CD Libraries, CD collections, AVW in a digital format, torrents, etc., related to the AVW.

I consider that AVW's being on a digital holder or its transmission in digital space is just another way of an AVW's existence. To be fixed AVW in a digital way is necessary to have the author's consent for use of this AVW.

When a public library, museum, archive institution do this fixation on the digital form for the purpose of conservation of cultural heritage, then author's consent is not necessary.

However, when a user, including an Internet supplier, creates a new digital format of the already existing AVW or made available the existing AVW for use by everyone, he must have received prior authorization from the author. He must have a prior permission by the author as a collective body.

The principle is that the author and the supplier are the two sides of the contractual relationship with AVW and its use as an object. This way of the economic realization of the AVW must bring revenue for the both sides, the author and the supplier. This income should be distributed between them. The particular way of the distribution of the forthcoming income from the AVW's use has to be fixed in the contract beforehand.

## **6. Duration of copyright protection on the audiovisual works**

Copyright protection is temporary. The principle is that copyright shall be protected while the author and seventy years after his death.

For works having two or more authors the term specified in paragraph 1 shall commence from the death of the last surviving author.

Copyright over anonymous or pseudonymous works shall be protected for fifty years after the works have been first made available to the public. In the event that within the said term the author's identity is disclosed, the provisions of the preceding article shall apply.

The terms mentioned in the preceding articles shall commence as of January 1 of the year following the year of the author's death, or, respectively, the year when the work was made, or made available to the public or published.

## **7. Legal defense against illegal use of the audiovisual works**

The audiovisual work could be used only under the permission of its author. Every use of the audiovisual work without permission is an infringement in the law.

These activities are called intellectual piracy or copyright infringement (CI). CI has grown dramatically since the late 1970s, as technology has facilitated the unauthorized duplication of copyrighted works. Copyright infringement surged in the entertainment industry after the advent of home video equipment. Initially, unauthorized recordings were made using hand-held video cameras to surreptitiously record movies shown at movie theaters.

In the 1990s, unauthorized duplication of AVW on CDs began to become an international phenomenon. It is estimated that over 100 million CDs with music and movies have been illegally reproduced for selling. The main reason for this is called Internet and the so called free use ,/personal mainly.

Not everybody sees copyright infringement as a problem. Some see it as a natural evolution of society in conjunction with the rise of the Internet, which fundamentally changes the way society operates.

Bulgarian copyright law includes the following ways for a defense: civil defense, administrative defense and penal defense.

1. Civil defense: in the case of infringement of copyright the author possesses the legal opportunity to claim before a court the following types:

1. The claim for a compensation for the damages;

but there is no sufficient information about the amount of the compensation, the author may demand the following:

- the revenues received as a result of the violation
- the value of the object of violation at retail prices
- an amount ranging from seventy levs to thirty five thousand levs.

2. The claim for restraining the illegitimate use;

3. The claim for seizing and destroying illegitimately produced copies of the work, including negatives, master copies, printing forms and others used for the purposes of copying;

4. The claim for seizing and putting out of operation the copying, decoding and reproducing equipment used exclusively for committing violations.

2. Penal-administrative defense:

Any person who has realised one or mixture of the following actions:

- Reproduces and distributes video media with recordings of films or other audio-visual works
- Reproduces and distributes audio media with recordings of works



- Organizes in any manner whatsoever public showings of films or other audio-visual works;
- Offers sound or video recording services to third parties consisting of the preparation of single copies of audiovisual works;
- Organizes live or recorded public performance or presentation of a work;
- Broadcasts by wireless, cable or other means audio-visual works;
- Publishes or distributes already published works

or other action from the granted exclusive author's rights shall be liable to a fine from two hundred thousand to two million leva, unless the violation is punishable by a more severe penalty and the object of the violation, regardless of whose property it may be, shall be seized in favor of the State and shall be delivered to be destroyed by the Bodies of the Ministry of the Interior.

There are some specifics when the case is second, subsequent or system violation.

3. Penal defense: Penal defense is under regulation of Penal Code, that differ three types of crime in the copyright's protection:

- Contrafacton: crime that includes fixing, reproduction, distribution, broadcasting or other action from economic author's rights without the author's legal permission; unauthorised use of one's own original; work.
- Plagiarism: the wrongful appropriation, close imitation or publication, of another author's language, thoughts, ideas, or expressions, and the representation of them as one's own original work. Copyright infringement is a violation of the rights of a copyright holder, when material protected by copyright is used without consent. On the other hand, the moral concept of plagiarism is concerned with the unearned increment to the plagiarizing author's reputation that is achieved through false claims of authorship.
- Intrusive authorship: under the force of the official state, e.g. the one of the boss, the dean or the manager as a part of the collective author's body. The mentioned person does not give a creative contribution to the released work.

Every kind of crime leads to fines and/ or imprisonment according the legal text of the Penal Code.

## **8. Consequences of the copyright protection on the audiovisual works**

Putting the audiovisual works under copyright law leads to the following:

- Every copying of the audiovisual works is treated as a law infringement and intellectual piracy;
- The author of the audiovisual works possesses the right to receive a compensation for own work in using;
- The company realizes the economic benefit from the product including the audiovisual works in trade;
- The company obtains goodwill in business field.

Advantages of this kind of protection are that there is no formalities and there is a long period of protection.

- no formalities

and

- long period of protection.

Copyright protection of the audiovisual works has disadvantages:

- only exactly copying of the audiovisual works is treated as a law infringement;
- The art concept could be modified easily and presented in other new form, which can be protected as an object of copyright law.

In the field of audiovisual works, we may discuss related rights of the performing artists, producers, legal users e.g. broadcasting organizations, internet suppliers and many others persons or organizations. Deeper presentation on this matter falls outside this paper's objectives.

# Freedom of the press in the eyes of Nigerian Law

---

Maureen Ifeyinwa Nwanolue &  
Edith Chinelo Ude-Akpe

---

## Introduction

Nigeria is the most populous country in Africa. It is situated on the Gulf of Guinea. It gained independence from the Great Britain in 1960. No country of the world can operate effectively without the functions of the press. The press history in Nigeria cannot be reviewed extensively without mentioning the colonialists' roles towards the development of the industry. The first generation newspapers in Nigeria were religious publications of different types, like Iwe Irohin, which was founded by Rev. Townsend hit the news stand on Dec. 3, 1859. Some other religious ones that kept close on the heels of Iwe Irohin were the newspapers founded by Rev. Hope Waddell: Calabar Observer which became the first newspaper east of the Nigeria, Unwamma Efik and Obupong Efik, all vernacular newspapers like Iwe Irohin also hit the news stand. Due to the fact that those first generation newspapers were published in vernacular prints, they only appealed to their immediate environs. Then, they quickly lost readership to other up standing newspapers which came in English language prints. Though they later started producing editions with English subtitles, their readership had already been lost.

Anglo African, a newspaper founded by Robert Campbell (another missionary), was more journalistic in its contents. It bore more stories, criticism and views. The newspapers helped to solve the problem of vernacular which the earlier newspapers were inclined to.

The colonialist religious newspapers however gave way to Nationalist Journalism. The printing school and presses which the colonial missionaries set up in Nigeria helped to equip those early Nigerian journalists in the art of print technology. The graduation of Nigerian-trainee print technologists, opened an express way to Nigeria Press. Nigerians who were lettered who had flair for journalism, joined force with their compatriots who were skilled in print technology, and together they created what has often being referred to as "era of the Nationalists press". It was the collective efforts of the Nationalists press that earned Nigeria her independence. Azikiwe (1964:17) stated ... "the early history of Nigerian press is identical with the intellectual and material development of the country. With the growth of education, we have been able to end up with more people

who can read and write". With the extension of our civilization and the expansion of our economy. We have been able to develop a better press and a higher caliber of journalists and printers, so that growth has been the ascent in the recent history of Nigerian press".

The press could be basically understood as an organization for the collection, transmission and distribution of new to newspapers, periodicals, television, radio and other journalistic and mass communication media. One may see them as independent companies whose serves are available to anyone who pays a subscription fee. The press come to be following a general need for faster transmission or dissemination of news.

In whichever manner the press is defined, it is important to note that press freedom should be separated from the freedom of the owners of the press. The law of Nigeria was made to repress the press and prevent criticisms of the government in power. All laws, whether it was the colonial seditious offences ordinance of 1909 or the precursor of the notorious public officers (Protection Against False Accusation) Dicers No. 4 of 1984 or even the Nigerian Press Council Act recently nullified by a Federal High Court, those laws were enacted to repress the press and prevent criticism of the government in power.

Again, the repressive laws are still being used by the State to harass and intimidate journalists. Under our so-called democracy in the fourth republic, journalists were charged with criminal sedition for publishing story indicating that presidential jets were not new but refurbished. Media organizations have been shut down by our democratic governments on account of publishing news that embarrassed governments. The closure of Channels Television and insider magazine recently demonstrated that qualitatively, there is little difference between the so-called democratic governments and military regimes.

### **Freedom of the press and section 22 of the 1999 Constitution**

Section 22 of the 1999 Constitution of Nigeria belongs to Chapter 2 of the Constitution. Section 22 compels "the press, radio, television and other agencies of the mass media to, at all time, be free to uphold the responsibility and accountability of the government to the people.

The provisions of Chapter 2 of the Constitution under which we have Section 22 are not actionable. Journalists or lawyers cannot cite any provisions of that chapter as defence in litigations on matters pertaining publications or broadcasts. Though, it gives the media the responsibility of holding government accountable to the people, it neither empowers nor protects the media to discharge its duty.

The 1999 Constitution has to a considerable degree, the same legal character with the 1979 and 1989 Constitutions. Section 3 (1) recognizes 36 states and the Federal Capital Territory, Abuja 1 Part 11, Section 4, 5 and vest legislative, executive and judiciary powers in the National Assembly, the president, the governors and the Courts respectively. Chapter 11 deals with fundamental objective and directive principles of state policy. While Section 38 of 1999 Constitution just emphasizes on freedom of expression. Although, the 1999 Constitution remains the workable functional legal document for the country, presently. The acceptability, legitimacy and credibility of the Constitution are being contested by some Nigerian intellectuals, politicians, and pressure groups. In the words of Ajaegbo (2004:47) "a veritable and lasting Constitution is one that derives its authority and legitimacy from the citizenry of a country, not only through consultation with strata of society but also by ensuring that their collective interests, hopes, yearnings and aspirations are firmly entrenched or embodied in the document. Only by faithfully doing this can our leaders and our democratic institutions truly launch this great country on the path of honour and respect, social progress, economic prosperity and political stability".

Perhaps, the reviewed 1999 Constitution and that of the Nigerian Press Council (NPC) drafted in (1999) are better than the previous Constitutions used in this country. A critical look at the two texts reveals that the provision on Freedom of the press did not stipulate any consequences for the violation and infringement of journalist's right to freedom of expression.

Again, the unpleasant implication of this is that freedom of expression for the press (journalists) is seen as the individual right to freedom of expression for respective journalists. Sections 21 of the 1979 and 22 of 1999 Constitution of the Federal Republic of Nigeria, have not in any way, "spoken" well of freedom of the press. Accordingly, Ezech (2003:90), asserts, the provision relating to the media in the new constitution are a rehash of those of the 1979 Constitution.

They simply imposed duties and responsibilities on media without granting the much touted fourth estate of the realm any right or privilege beyond the general right to freedom of expression guaranteed every person in Nigeria. This is why no government in Nigeria has deemed it necessary to respect the press constitutional right to freedom of expression. In continuation, the Constitution of Nigeria, like any other country's like any other's country's is saddled with the responsibilities of making the laws that guide the citizenry's socio-political and religious inter-relations.

According to Chapter 11, Section 22 of the 1999 Constitution also serve as Federal Republic of Nigeria (1999:13) the obligation of mass media is entrenched thus: the press, radio, television and other agencies of the mass media shall at all

times be free to uphold the responsibility one accountability of the government of the people.

### **Restrictions to freedom of the press**

More often than not, press laws are difficult to describe. Hence Agbaje, (1983:64) argues that the reason is because of the complexity of the ever changing society in which they are found. He describes myriad competing influences on how the press constructs legitimacy for the Nigerian people. Agbaje describes it as a “battle field of representation”. He goes on to describe the problem being exacerbated by the colonial heritage and non-Africans trying to explain the realities of the nation’s complex social structure.

Over the years, the Nigerian government has shown negative attitude and restriction of press freedom. On March 28, 1995, the Information and Culture Minister, Walter Ofonagoro told reporters that government is determined to ensure that the private press is “whipped into line”. Few days after, during a visit to Vanguard Media Limited, Apapa, he complained of what he described as sensational headlines and warned that “freedom is not synonymous with license”. Also the Foreign Affairs Minister, Tom Ikomi warned during an interview on BBC that “any journalist who commits a crime under the guise of practicing his profession will not be spared”.

This ongoing battle of ideas can be seen throughout Nigeria’s history. In 1984, the Buhari Military junta scored a milestone with the promulgation of the infamous Decree No. 4 designed to clip the wings of the press. The Decree was solely meant to protect government officials from embarrassing press reports irrespective of the truth of such reports.

Government involvement in the affairs of the press is not limited to obnoxious enactments. It also tries to influence and in fact determines who occupies the leadership position of the National Union of Journalists (NUJ) at all levels. On July, 21, 1993, the government churned out the Treason and Treasonable offences Decree and Offensive Publications (prescription) Decree 35 of 1993 with the following seven media houses, National Concord, African Concord, The Punch, Daily Sketch, Observer, Abuja News Day and Ogun State Broadcasting Corporation (which was later re-opened after 24 hours).

On April 6, 1987, the government proscribed News Watch Magazine for six months, for publishing the reports of the cookey-led political Bureau before government’s white paper was issued on it. It was immediately backed with Decree No. 6 of 1987 known as “News Watch (proscription and prohibition) Decree. Following this, news watch’s account was frozen by the government and the two

editors were arrested. On March 8<sup>th</sup>, 1991 Lagos News Magazine was sealed off by security agents and its editor, Kolawale Alabi detained for a story published on the day's editions of the paper entitled "IBB, Maryan involved in Jennifer Madike's story. It linked the then first couple with drug trafficking.

Abacha's regime was not better off either. Many instances of anti-press posture abound. For instance, on April 7<sup>th</sup>, 1994, the news watch fell victim of government sledge hammer. Why? It published an interview granted by Major David Mark on activities of the government. Also, in 1995, the editor of the Sunday Magazine, Mrs. Chris Anyanwu among others was arrested and imprisoned for an alleged complicity in connection with the so-called aborted coup allegedly organized by Obasanjo against Abacha's regime. She was released sometime in 1998 when General Abubaka succeeded the late dictator Abacha.

Nwanolue (1998: 225) in support of this stated that: a democratic government that is accountable to the people will respect the rule of law and fundamental rights of the citizenry, including the rights of the press together, process and disseminate information without hindrance.

In spite of the framework that has been set in place for press freedom, Nigeria continues to be unable to publish opinions freely. Both during periods of civilian rule and military dictatorship, the nation never experienced a complete assurance of a free press. Government philosophy and document may state that press freedom exist, but in the day to day affairs of life such freedoms fluctuate widely.

In Nigeria, laws, ordinances or Decrees or even Acts are promulgated to restrict the press from expressing certain formation on matters considered inimical to the authority.

### **Problems of nigerian press**

Due to the instability of the various government over the years, the relationship between the state and the press has fluctuated, as a result of number of factors. At times, there have been some moderate considerations given to press freedom, while other times, journalists disagreement with the government manifest itself in blatant violence.

In reviewing the history of the nation, the long-term trend has been that of the repression of free press. The constitutional privileges that are in writing have simply not been experienced by the real world of daily Nigerian life. On the surface, it appears that there is much diversity of expression due to the large number of media outlets in the nation. However, when a closer observation is made, the complex political and social systems of the nation are the context which these media organizations operate and it is discovered that the "societal watchdog"

function of the press does not operate in reality in Nigeria as it does in more free and open society.

The committee to protect journalists, a New York based nonprofit, nonpartisan organization that monitors press freedom globally, reported serious reservations about Nigeria's government press relations following the election of former president Obasanjo. CPJ noted that "although a new constitution was promulgated on May 5 (1999), it was modeled largely after 1979 Constitution and offered the media no specific protection".

About 20 anti-media decrees were identified by CPJ in the amended Nigeria Constitution of 1999. One measure was repealed, the one that called for newspapers and magazines to register with the government. Later it was surreptitiously introduced as the Nigeria Press Council (Amendment) Decree Number 60 of 1999.

While press attacks decreased significantly after the transition from military to civilian rule, there remained reported abuses. CPJ reported after the election, police raided the editorial offices of the independent Lagos Newspaper, the News and arrested several employed journalists (NUJ), was arrested. It was politically motivated. Even government owned media employees experienced harassments. Two reporters for the state owned newspaper the observer were suspended for publishing statements considered to be critical of the election process made by international observers.

Media freedom suffered a setback in 2008 when a freedom of information BILL (FOIB) in the parliament, since 1999, failed to scale through the committee stage, despite strong support from domestic and international media groups. Although the 1999 constitution guarantees freedom of expression, of the press, and of assembly, the state often uses arbitrary actions and extralegal measures to suppress political criticism and expression in the media. Criminal prosecution continues to be used against journalists covering sensitive issues such as official case, separatist movements, and communal violence. In addition, Sharia Islamic Law in Northern states impose severe penalties for alleged press offences.

Various security agencies used arbitrary detention and extrajudicial measures in a muffle political activism and restrict press coverage that was perceived as critically related to sensitive issues. Such include official corruption, violence in the oil-rich Nigeria. In January, 2008, security agents in Akwa Ibom State detained some journalist and instituted sedition charges against the local newspaper distributors and a newspaper chairman with a story alleging that the state government had tried to corrupt individuals. Again, four U.S. film makers and one Nigerian were arrested while shooting a documentary of Niger Delta Region. According to the



committee to protect Journalists (CPJ), the spent a week in custody without being charged. In August of the same year, freelance U.S. filmmaker Berends and his Nigerian translator, Samuel George, were detained by state security service in Port Harcourt. Berends was released after three days, but was forced to undergo questioning before being deported, George was held for five days and interrogated. The SSS agents, in September of the same year, temporarily close down the Lagos and Abuja officer privately owned channels TV Station and detained at least four staff members who aired a fabricated report that president Umaru Yar'Adua might step down with reason. Later, the SSS detained the publisher of the newspapers leadership Isaiah, and questioned him for two days, regarding a report alleging that the president is critical ill. A presidential directive instructed the police to arrest Nda-Isaiah along with editors and a former associate editor of the paper for "defamation of character and injurious falsehood". The journalists were released on bail pending the determination of suit in 2009.

Some Nigerian journalists were murdered in 2008 for reasons that remained unclear to people. In August 2009, Paul Abayomi Ogundeji, a board member of the private daily *This Day* was stabbed to death in a sub-office in Lagos. Two Nigeria reporters were shot by police officers, according to the U.S. State Department. In October of the same year, Ephraim Audu, a radio journalist with the Nasarawa State Broadcasting Service, was assassinated by gunmen near his home in Lafia. Investigations into both murders were still pending. Physical violence against journalists remained a common occurrence, particularly those covering public protests, political rallies, or abuses of power by security. For Dave Amusa, the Rivers State correspondent for the *National Mirror*, was beaten while attempting to enter the independent Electoral Commission offices in Port Harcourt, to get reports of council poll results. Also, security agents assaulted a channels TV, police officers in Lagos reported beat three print journalists who were covering rally by the opposition action congress party in September.

Despite the transition from military to civilian rule in 1999, clampdown, assault, beatings, unfair arrests and police raids against producers of print media have continued. Between June 2002 and September 2003 alone Media Right Agenda (MRA), a Lagos based nongovernmental organization which promotes press freedom and freedom of expression, recorded more than fifty cases of reported abuses against journalists and other violations of freedom of expression.

The media watchdog reporters without borders has just listed Nigeria Police Force as the leading abusers of journalists' right. On Saturday, April 24, 2010, Edo-Ugbagwu, a judicial correspondent of the *Nation Newspaper* was murdered in Lagos. Also, Godwin Agbroko and Abayomi Ogundeji of *This Day Newspaper*,

Omolu Falabi Bayo Ohu of the Guardian were all brutally killed in Lagos by unknown gun men recently.

## Conclusion

An urgent call is hereby made to the Senate and House of Representative to pass the freedom of information Bill (FOIB), which when fully implemented, will help to strengthen democracy, ensure transparency, accountability, good governance and the rule of law in Nigeria. When press freedom is accorded its due position, it will be a good test for democracy, rule of law, due process as well as re-branding.

The abolition of press repression is not just a legal project but also political. It has deviated from a mere reform to a revolutionary reconstitution of the country. We also wish to project that political project will touch on the electoral system to ensure that votes count. It will also have to de-monitize the electoral process so that people would not have to steal public funds to usurp powers.

Lawyers and allied groups would also need to be a lot more proactive to come up with suggestion on law reforms, such that would encourage access to information and freedom of the press. May we clearly state also, that freedom of the press cannot stand or succeed where other fundamental rights are trampled upon. When it stands, it will be fortified when other numerous conflicts are resolved.

Nwanolue (2004: 225), said as Nigeria seeks to achieve a true freedom of the press, there is need to terminate the culture of secrecy that has become endemic in government circle. It is only in a democratic atmosphere that press freedom can thrive a democratic government that is accountable to the people will respect the rule of law and fundamental rights of the citizenry including the rights of the press to gather, process and disseminate information without hindrance.

All these killings and the reluctance of the national assembly to pass the freedom of information bill have further raised the question of press freedom once more in Nigerian democracy. The assault on the press is a fundamental breach on democratic norms.

## Recommendations

Based on the above discussion the freedom of the press in Nigeria, we make the following recommendations to better the lots of journalists in Nigeria. They include:

1. For a country's media to be truly free there must be the right mix of the social, political and legal environments. A deficiency of any of these setting will compromise the total and true freedom of the media in the country. The foundation

for a free press and a free society is possible when the right laws are in place and there are complaint to the rule of law.

2. Article 19(2) of the international convention on civil and political right (IC-CPR) in recognizing of expression and the press states: Everyone shall have the right to freedom of expression, this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." Therefore, Nigeria government is requested to observe the rules of the above article 19(2).

3. A Freedom of information law is necessary and vital tool for fighting corruption in public and private sectors. This, if observed, would ensuring social, economic and political development through the availability of useful information in Nigeria.

4. Finally, the press is requested to embark on a more objective, investigative, informative and educative journalism. This would balance their activities and always speaks for them whenever the government raises to victimize them in Nigeria.

## Reference

Agbaje, Adigun A. B., *The Nigerian Press, Hegemony and Social Construction of Legitimacy 1960 – 1983*, Lewiston, NY: Edwin Mellen Press, 1992.

Ajaegbo D. I., *The History of Constitutional Development in Nigeria*, Onitsha: West & Solomon Corporate Ideals Ltd, 2001.

Daniel, Clifton, (ed.), *Chronicle of the Twentieth Century*. Mount Kisco, NY: Chronicle Publication, 1987.

Ezeah O., *Mass Communication in Nigeria. A Book Reading*, Enugu Forth Dimension Publishing Co. Ltd. 1999.

Ofor Okey C., *Nigerian Press: Review Trends and Prospects*, 2004.

Nwanolue B.O.G., *Government and Mass Media in Nigeria*, 2006.

All Africa Com. 3 May 2002. Available from [www.allafrica.com](http://www.allafrica.com). The central intelligence Agency (CIA) World Fact book 2001. Directorate of intelligence, 2002 Available from [www.cia.gov](http://www.cia.gov).

Constitutional rights project. 31 March 2002, Available from [www.Crp.org/ng/main.htm](http://www.Crp.org/ng/main.htm).

Freedom of the press in Nigeria – some fundamental issue – 3 by Bamidela Aturu Sept. 10, 2010 – Vanguard online from [www.vanguard.com/2010/09](http://www.vanguard.com/2010/09).

Onadipe, Abiodun. Nigeria and Democracy: Third time lucky Contemporary Review Company Ltd 30 March 2002. Available from [www.finderticles.com](http://www.finderticles.com).

"News and media". Nigeria infonet. 23 March 2002. Available from [www.nigeriainfonet.com/directory/newmedia.htm](http://www.nigeriainfonet.com/directory/newmedia.htm).

Nigeria Press, Media, TV, Radio, Newspaper – Newspaper, television, news circulation. Available from [www.pressreference.com/ma.no/nigeria.html](http://www.pressreference.com/ma.no/nigeria.html).

"This is NBC" 30 March 2002. Available from [www.nbc-org/nbc-ng/org.html](http://www.nbc-org/nbc-ng/org.html)

# Profiling and manipulating human behaviour: a core contemporary privacy concern

---

---

Alan McKenna

---

---

“The more a man may live according  
to his own inclinations,  
the more he is free.”

(Peter Forsskål – Thoughts on Civil Liberty: 1759).

## 1. Introduction

A feature of recent years has been the almost incessant stream of privacy related stories that have been reported by both traditional media and new media sources, with rarely a week going by without at least one new privacy related story emerging. Such stories arguably either individually or cumulatively add to the perception that the current era appears to be one in which privacy violations, or potential violations, are endemic, with our private lives and personal information being beset by a plethora of watching eyes, be they physical, mechanical or digital.

With such concerns over privacy violations what are the specific harms that emanate from such intrusions into our personal lives? With so much written about potential or actual privacy violations, at times it appears almost taken for granted that this is a negative thing and as such there is perhaps no need to elaborate further as to the specific harms we might face when our privacy is violated. Indeed, one American journalist recently wrote how after years of trying to protect his privacy, he is now literally going to go with the information flow and abandon his attempts to protect his online privacy as it could be that the benefits of doing so may outweigh any downside (Hill, 2011). Perhaps Hill's conversion can in some ways be seen to reflect a new culture that is developing with the proliferation of information and communication technology (ICT) devices, and how we communicate and inform others about our lives. Anyone who travels on a train in the UK today for instance will listen to a varied number of telephone conversations during their journey, in which the speakers provide without any apparent concern, all types of personal information. Travel back in time twenty years, and the same passenger would witness their fellow passengers talking in mostly hushed tones to each other, providing little clue as to what they were talking about.

Privacy arguably however remains fundamentally important and will continue to do so despite how the new technologies have given us the possibility to communicate and share information more readily, with one commentator arguing its importance can be seen as lying in Man's DNA itself, for paradoxically whilst we are social beings who like the company of others and are inquisitive to know what fellow humans are doing, we also like our own private space, feeling inner security in being able to go home and draw the curtains on the world. (Melville-Brown, 2008). As such, of course, it can be said that a fundamental feature of the human form is our right to personal autonomy. In their famous paper on the right to privacy, Samuel Warren and Louis Brandeis refer to American Judge Cooley's phrase, 'The right to be let alone'. (Warren & Brandeis, 1890). This phrase perhaps provides us with an underlying essence of why privacy matters. Not just with the guaranteeing of our personal autonomy in respect of, for example, being able to withdraw from the world and its gaze at our choosing, but more than this, in not having our lives in ways we have little or no control over, directly interfered with by others, whether they be individuals, corporations, or states, when they obtain and use information specific to us. In 1960 the American academic, William Prosser, identified four distinct ways in which he considered personal privacy could be infringed: (i) by intrusion upon a person's seclusion or solitude, or into his private affairs; (ii) by public disclosure of embarrassing private facts about a person; (iii) by publicity which places a person in a false light in the public eye; and (iv) by appropriation, for the defendants advantage, of a person's name or likeness. (Prosser, 1960).

Unsurprisingly, it has been argued that Prosser's understanding and interpretation of privacy violations, in coming from a pre-digital age, are insufficient for today's world, in that digital technology has clearly extended the situations and forms by which personal privacy can be violated. (Keats Citron, 2010).

What this paper seeks to consider is that in looking at the changing developments relating to the potential privacy implications that the advent of digital technology has brought about, the possibility of the carrying out of highly sophisticated profiling of individuals now exists, and, as a consequence of such profiling possibilities, it may be argued that it is not only potentially feasible to predict human behavioural patterns by use of the information obtained, but also to actually take the next step and, in theory, manipulate human behaviour. In looking to address such issues, whilst to date the primary focus of attention in respect of one particular use of such profiling techniques relates to behavioural advertising in the on-line world by commercial organisations, it is important to be aware that although such practices are being used from the commercial context of being able to sell more goods and services, without doubt the privacy invasive technologies being utilised can be used by other types of parties, most obviously governments and

related governmental organisations for alternative purposes, and like commercial operators their aim would be to induce change in individuals' behaviour.

In looking at how such challenges have to date been addressed and how they might be met in the future, it is necessary to consider the full range of protective provisions, be they regulatory, technical or, for example, educational, as arguably ultimately no one single protective course will by itself be sufficient to counter the challenges faced. Naturally, the primary focus has been on regulatory provisions, and from a global perspective Europe has been at the forefront of much of the analysis and regulatory development that has taken place in seeking to address the new privacy related challenges that have emerged. It is perhaps unsurprising and appropriate that the very first data protection law created anywhere in the world came from within Germany, when in 1970 the German state of Hesse sought to address concerns that had emerged over the surveillance implications for the citizens of Hesse, whose sensitive personal data was being collected and stored on public databanks. (Simitis, 2010) (Burkert, 1999). It is appropriate, of course, that such legislative leadership should emerge from Germany when we reflect on how the Nazi regime had used detailed information collection systems to help facilitate control and mass murder.

Reflecting a general trend of growing global interconnectedness in terms of not only communication links, but also of general reliance, there have been calls for comprehensive global privacy instruments to be developed and adopted in order to protect individuals' privacy. (International Data Commissioners, 2009). Whether agreement could be reached on a binding comprehensive instrument that is fully enforceable throughout the world, would seem currently a difficult prospect.

Whilst much of what will be discussed concerns the use of personal information by commercial operators, the role of the state as already alluded to requires close consideration, and despite the positive recent example of the use being made of information and communication technologies in the form of social media to help facilitate the protests that led to the collapse of a number of despotic regimes, undoubtedly states whether they be undemocratic and democratic in nature, will develop their understandings of the new technological systems and potentially utilise them in ways that could ultimately inhibit personal rights and freedoms, and this is something which we must be acutely aware of and be prepared for.

## **2. The developing use of profiling within the context of a growing information dependent society**

For more than twenty years western governments have been keen to locate the development, collection and usage of digital information at the heart of their pol-

icy agendas, with an overarching aim being the creation of what has variously been labelled an Information Society, Knowledge Society or Digital Economy. Whilst recognising the importance in part of the social aspects of such a development, much of the primary focus has concerned the economic potential of using the new technologies and digital information. This can of course at times lead to problematic conflicts occurring between the aim of facilitating the creation of economic wealth and economic development, in contrast to other more societal specific goals and values. We should perhaps locate our discussion within this context, with tensions between such issues intensifying in times of general economic difficulty.

The notion of profiling can be seen to occur in a wide variety of contexts in modern life, and arguably Man has in fact engaged in acts of profiling since his/her first emergence, profiling both his/her fellow humans and the environment in which he/she exists. At its heart the aim of profiling may be said to be the obtaining of information and knowledge.

In a modern context Hildebrandt considers that profiling can be seen as:

'The process of 'discovering' correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to indentify a subject as a member of a group or category.' (Hildebrandt 2008:19).

Of itself profiling arguably should neither be seen as bad nor for that matter good. (Gutwirth and De Hert 2008: 289). What is key, however, in assessing its nature is how it is carried out and for what purposes it is carried out. The knowledge that is generated by profiling, Gutwirth and De Hert have termed non-representational, as the profiles are said not to be about representing a current state of affairs, but look rather to predict future behavioural characteristics based upon the past actions of the parties that are subject to the profiling. (Gutwirth and De Hert 2008: 289). On a general level, the undertaking of surveillance activities, whether by companies or governments, in order to profile specific individuals or groups has been called social sorting, the essence of which is to classify individuals or groups according to varying criteria. Of course, the sorting of populations is a common feature of modern life, with examples being sorting to decide who should be taxed at a particular rate, or who is eligible for a specific benefit. But whilst some forms of social sorting based upon profiling activities may be of fundamental importance in the effective running of a modern society, we must remain vigilant as some social sorting can be tantamount to discriminatory practice. (Ball et al 2006: 11.4).



With the use of information and communication technologies (ICT's), Van der Hof and Prins have described how what they consider to be a fundamental change has been taking place in the consumer marketplace, contrasting the early 20<sup>th</sup> century notion of mass production based upon similarities between consumers that led to limited choice against the contemporary idea of mass individualisation, in that goods and services are now becoming tailored to the desires of consumers. In order to achieve what has been generally termed personalisation of service, companies use ICT's to select, filter and classify user information. (Van der Hof and Prins, 2008: 112-113). This may seem unproblematic, even perhaps clearly beneficial to the individual consumer, in that his/her desires are being specifically catered for. However, Van der Hof and Prins point to what they term the dark side of personalisation, raising a number of concerns over potentially detrimental impacts for both the individual and society in general. Of fundamental concern for them is the ultimate impact on individual autonomy, and whether personalisation can lead to discriminatory practices when such detailed information has been collected. (Van der Hof and Prins, 2008: 115-124). We can see a facet of personalisation with the emergence of individualised advertising. The growing development of ICT's have enabled commercial enterprises to develop a form of advertising that moves away from the traditional standard of a generalised advertising campaign to one that targets individual, based upon the information and knowledge that advertisers accumulate on individual consumers' interests via profiling; this has become known as behavioural advertising, the provision of your own personal online adverts. It is quite noticeable and for some people probably quite alarming how adverts for products that you may have been looking at on one particular website, then appear persistently to follow you around the web, almost demanding your attention.

Attempts to use an individual's information and behavioural patterns should not be seen as unique to commercial enterprises, for it does not take too much imagination to envisage its use and development for governmental purposes. The influencing of behaviour by rulers/governments naturally has a very long history. State controlled violence is an obvious extreme example of a long standing behaviour influencing mechanism. Today, governments in democratic states primarily rely upon legislation, taxation, and information provision in seeking to influence behaviour. However, there appears a growing recognition within governments that there are alternative strategies that could be employed, which may be cheaper and potentially more effective. An example from the United Kingdom of such recognition came in 2004 when the UK Prime Minister's Strategy Unit undertook research into how government policy could be enhanced and public behaviour positively influenced by the use of sophisticated psychological techniques. (Prime Minister's Strategy Unit, 2004). A further report commissioned by

the UK government was published in 2010. Its authors, The Institute for Government (IFG), in asking why it was necessary to consider alternatives to the traditional methods used to influence behaviour, argued that behavioural theory provided two reasons: firstly, that the impact of existing tools could be greatly enhanced by new evidence about how human behaviour is influenced; and secondly, because there were new and potentially more effective ways that 'government could shape behaviour.' (Institute for Government 2010: 8). Utilising the science of behaviour, the IFG argue that the acts of individuals are often influenced by sub-conscious cues. A technique they term Priming shows that individual's subsequent behaviour may be altered if they are exposed to certain sights, words or sensations. Thus, if people are pre-primed by cues, they will behave differently. (Institute for Government 2010: 24). The IFG recognise that the techniques being considered may be utilised in a way in which individuals may not appreciate that their behaviour is being targeted and changed, or at least in how it is being changed. This could of course lead governments to face charges of manipulation. (Institute for Government 2010: 66). Consequently, this would bring into play important issues such as infringement of personal autonomy, freedom of choice and control. Arguably, if such manipulative techniques are to be allowed to be used at all, then it would be appropriate if this occurred with the prior knowledgeable approval of those whose behaviour is to be targeted for change.

Use of new types of psychological techniques to influence behaviour clearly raise matters of fundamental importance, but it can be appreciated that governments when, for example, faced by a challenging financial environment, are likely to look for more effective and less costly ways to influence behaviour. Whilst all the ethical considerations involved may be outside the scope of the parameters of our discussion in this paper, what does bring the issue within its scope is if it can be argued that an individual's behaviour is at risk of infringement by the use of such manipulative techniques. Thus, for example, it may be asked whether our personal information is being used in a way that will facilitate the manipulation of our behaviour and is this ethically acceptable, both to the individual in question and to society as a whole?

In looking to achieve more effective use of such techniques, by effective I mean, of course, those that actually can be shown to change behaviour, with it being recognised that humans do not always respond in what may be seen as a rational way by doing unexpected things (Institute for Government 2010: 8), the likelihood is that it becomes important to adapt such techniques to meet individual personalities; and with the advent of advanced digital technology and profiling possibilities, this makes such effective use even more likely.

Reflecting genuine belief in its potential, following on from the IFG 2010 Report, the UK Government has now created within its Cabinet Office a seven strong Behavioural Insights Team, which includes academic experts on behavioural sciences. Cabinet Secretary, Sir Gus O'Donnell, who heads the team argues that 'many of the most pressing public policy issues we face today are equally influenced by how we, as individuals, behave. We can all cite instances in which we know that we should act differently in our own self interest or in the wider interest, but for one reason or another do not. The traditional tools of Government have proven to be less successful in addressing these behavioural problems. The Behavioural Insights Team has been established...to help the UK Government develop and apply the lessons from behavioural economics and behavioural science to public policy making.' (O'Donnell, 2010). It should be noted that the UK is not alone in Europe in setting up such a unit, with the French Government also working on such projects. (Franco-British Council, 2010).

Whilst governments may be newcomers to the field, it would be extremely surprising not to find the advertising industry at the forefront of the field, as, of course, with the ceaseless pressures of the competitive commercial marketplace, advertisers and marketers will look for any advantage to put them ahead of their rivals. Historically, advertising has been conducted on what may be now considered as a rather random non-cost effective basis, in that the vast majority of people who encounter a particular advert are likely to have little or no interest in the advert and will not be influenced by its message. Now with the emergence of behavioural targeted advertising, on the basis of information collected directly, targeted individuals are far more likely to be responsive to the specific adverts directed at them.

Understandably, it has been argued by legal academic Tal Zarsky, that a commonly used advertising model which sees optimal advertisements as being those which cross an individual's barriers of perception, capturing their attention and affecting their comprehension, can be achieved with greater success in the on-line environment with content based upon personal data specifically tailored to individual characteristics detected via profiling techniques. The crossing of an individual's barriers of perception implies that the relevant message enters that individual's sensory register. In a similar way to what was discussed in terms of the technique of Priming, here the preferred form of perception refers to the shapes, colours and sounds which are optimally received by the specific individual. Being able to capture an individual's attention requires information to be obtained as to that individual's interests and on gaining access to their attention, the final task is to cause that person to comprehend a specific point, which naturally would be that they should consider buying a particular product. (Zarsky 2006: 216-217). An effective message from an advertisers' perspective could at times

mean an unfair and manipulative message from that of its recipients. Again, of course, we run straight into questions of fairness and infringement of personal autonomy. (Zarsky 2006: 219). Where, it might be asked, is the boundary to be drawn between what is a fair attempt to influence and activities which are to be considered unfair and manipulative? (Zarsky 2006: 220). In contrasting the changing advertising landscape, it is argued by Lessig that there is likely to be general scepticism about the power of general television advertising to control people's desires, as the motives are so clear. But he questions what happens when the motives are not so clear cut, when a system appears to know what you want better and earlier than you do, how is it possible to know where the desires really emanate from? (Lessig, 1999: 154).

It is Zarsky's belief that the key to mitigating potential consumer detriment caused by personal profile constructed advertising messages, should be based upon two notions: firstly, by providing consumers with notice as to the tailoring of such individualised communications, and how their personal information is used to achieve this; and secondly, by assuring that consumers receive a balanced mix of messages. (Zarsky 2006: 221). Whilst providing notice to consumers of tailored advertising appears an appropriate solution, it should be asked whether mere notice of such advertising is potentially insufficient, and that for consumers to have a real appreciation of what is taking place they would need to be clearly made aware of precisely what is taking place. (Office of Fair Trading, 2010: 52). Pan-European self-regulatory initiative for online behavioural advertising has just been launched. This is said to seek to enhance transparency and consumer control, enabling the consumer by clicking on a standard form and strategically placed Icon they to be provided with further information about behavioural advertising and the way they can manage their information preferences. (Internet Advertising Bureau, 2011). An additional suggestion that might be added when consumers click on the Icon, is providing the option of seeing a short film on the nature of the advertising that is being encountered, as this may prove far more illuminating in explaining the precise nature of the advertising that is taking place.

### **3. Profiling Technologies**

If anything is certain about the technologies that can be used for surveillance and profiling purposes, it is that they are going to become ever more pervasive and powerful, as clearly technological development is not going to stand still.

One of the key technologies that enable online profiling and behavioural advertising to take place, and which have continued to evolve since they first appeared are cookies. Cookies are text files which are placed on a user's machine by a web server, enabling the server to recognise a particular visitor to their website when

they return to the site, this being considered of particular importance in respect of online transactions where ongoing steps need to be undertaken and the server needs to be aware of previous actions.

When studies found that over 30% of users were deleting cookies from their machines each month, this finding proved problematic for advertisers, as it meant that consequentially there was an overestimation of the number of true unique visitors to websites, with subsequent overpayment being made by advertisers to websites. As a consequence and desiring greater tracking reliability, the advertisers sought new solutions. (Soltani et al, 2009). What resulted were far more powerful, privacy intrusive cookies being developed. These newer forms of cookies have been variously called supercookies, Flash cookies, evercookies or ubercookies, having far greater storage capacities than normal cookies; and being stored outside the browsers puts them outside of the user's browser control. They can be difficult to erase, and some types actually have the capacity to regenerate deleted cookies. (Tirtea et al, 2011). Furthermore, such cookies have the capacity to follow and identify users across multiple different sites.

Highlighting how pervasive they have become, research carried out in 2009 on U.S. websites, found that 54 of the top 100 U.S. sites placed Flash cookies on users' machines. On several of the sites it was found respawning was taking place via the Flash cookie; that is after the user deleted the HTTP standard cookie, it was actually being recreated by the Flash cookie. Another even more recent investigation carried out by the Wall Street Journal in the United States, found that some large U.S. websites were installing more than 100 tracking devices including cookies on visiting users' machines. The 50 most popular U.S. websites were examined to measure the quantity and capabilities of the tracking devices, and it was found that the 50 sites installed a total of 3180 tracking files on the test computer. They discovered that some of the tracking files had the capacity to record an individual's online keystrokes and to then transmit the text back in order for it to be analysed for content, tone and clues as to an individual's social connections (Angwin, J and McGinty, T, 2010).

For the purposes of profiling it is important to appreciate that, whilst significant data can be obtained via the use of just one type of ICT, if such data can be combined with data obtained via other types of ICT's, this could significantly increase the potential strength and depth of the overall profile achieved. Another of the technologies that has drawn attention over its profiling possibilities is data mining, which in essence is via the use of algorithms, a way by which large datasets can be analysed in order to extract previously unknown and potentially useful information. There are said to be two distinct approaches to data mining – descriptive data mining, the goal of which is to discover unknown relations between dif-

ferent data objects; and, predictive data mining, which aims to be able to make a prediction about events, so this might, for example, take the form of predicting whether an individual fits a previously established profile (Schermer, 2011: 45-46).

Whilst data mining has been highlighted for concerns over its implications for personal privacy, a counter argument is that the technology by itself is not the problem, it is how it is utilised the potential problem, and with the technology being of great value, there are concerns that privacy worries could impact upon its future development and use. Clifton et al argue that the negative association with privacy infringement is unfortunate in that with growing amounts of data being created by various bodies, such volumes of data instead of offering greater insights can actually hinder overall understanding, without there being the capacity in place to be able to condense and analyse it. Furthermore, in an overt attack on lack of government/public finance for research into such fields, they raise the spectre of a consequential negative privacy impact due to what they claim could result, that researchers will turn to private money where there might be less concern over privacy, and also less information about data mining subsequently being made public with knock on privacy impacts (Clifton et al, 2006: 191-193).

Schermer has argued that when it comes to data mining and profiling, especially when carried out via an automated process, data protection law does not provide adequate protection. It is his belief that there exists a lack of co-operation between the data mining community and data protection community, and with the law being based primarily on ex ante protection, there is little by way of ex post protection mechanisms. As such he feels there is a need for greater ex ante screening of data mining applications for potential risks and ex post checking of results, as currently data mining is a black box process for outsiders. In looking to provide adequate protection, the recent initiative of developing privacy by design has an important role to play, with, for instance, the creation of Privacy Preserving Data Mining (PPDM) algorithms being used to protect personal data. Schermer however, feels additionally it is necessary that there also are put in place mechanisms to detect improper use of data mining and profiling in policymaking, which may take the form of an oversight committee made up of a mixed discipline cohort (Schermer, 2011: 49-52).

Information for profiling purposes is also obtained from what we may term the physical world, as opposed to the digital online world, although clear crossovers can be seen to exist. In the physical world, the most well-known and abundant technology that is used for profiling purposes are CCTV systems. The United Kingdom perhaps has the dubious reputation of currently possessing the most CCTV cameras of any country in the world. An early use for such cameras was to protect retail stores from shop lifting. The in-store security camera could how-

ever soon be joined by a far more powerful privacy intrusive off-shoot. The Chief Executive of U.S. shopping marketing company, Shopper Sciences, provides an interesting glance into what may be a future feature of physical retailing when he argues, 'New technology can use digital cameras to record shopper reactions to in-store marketing. This gives marketers real-time feedback on how they are responding and interacting with displays. More than simple traffic and monitoring software, the next generation of in-store analysis tools tell us emotional and physiological responses as well. Digital analytics company Affectiva offers real-time emotional tracking that can actually measure facial responses, head movements, and even heart beat as shoppers interact with products, kiosks, and retail displays.' (Ross, date: 9). A further example highlighting a growing interest in what may be called machine based visual intelligence, the United States Defense Advanced Research Projects Agency (DARPA), the Agency which began the research into what ultimately became the Internet, has this year begun a new project called Mind's Eye. The aim of the military project is to move past the current state of the art in machine vision technology in which a range of objects and their properties can be automatically recognised, to seek a machine capability that currently only exists in humans, the visual intelligence, to actually understand and analyse a particular scene. (DARPA, 2011). It takes little imagination to see that if such technology is successfully developed that it is likely in some form to move from the field of military usage to be used in commercial contexts, with undoubted potential privacy implications.

Until now the most significant way in which traditional retail stores have obtained information about their customers shopping habits has been via the use of loyalty cards. Of course, it must also be remembered that traditional retailers will also have an online presence potentially providing additional information about their customers. But Ross holds out the possibility of even more enticing information collection that traditional retailers may be able to obtain when he poses the rhetorical question, 'What if you could get online style metrics in-store? How powerful it would be to identify and track individual shoppers throughout their shopping journey, just like we do online, giving them customized offers, discounts, and communications as they move throughout the store. And then to know where non-buyers went after leaving the store?' (Ross, page 2). The emergence of two further technologies, Radio Frequency Identification (RFID) and Global Positioning Systems (GPS) in combination with shoppers' smart phones, now allow retailers potentially to identify shoppers when they enter a shop (Ross, date: 8).

RFID and GPS technologies provide the additional dimension to profiling technologies in that they produce location based tracking information. Highlighting how potentially invasive the information obtained via GPS can be, Malte Spitz, a

German politician recently discovered that over a six month period from August 2009 to February 2010, his mobile phone company T-Mobile via GPS technology had recorded his precise location more than 35,000 times. What many people do not realise is that every few seconds mobile phone companies determine the nearest mobile phone mast to their phone to ensure efficiently routed calls (Cohan, 2011).

GPS and RFID technologies are seen to be complementary in enabling instantaneous identification of location and therefore the tracking of people, vehicles or goods, with GPS providing a more general location and RFID a far more accurate one, but RFID being more restricted in terms of when tracking is possible than GPS currently. An RFID tag when it passes within range of a compatible RFID reader via use of radio signals will record the time and location. (Monmonier, 2006: 75-76). Much of the early use of RFID came in respect of general stock movement management systems, with no related privacy implications, but there has become a growing awareness that they can be used in situations where there certainly will be privacy implications – active tags inserted into goods that theoretically could be tracked to a person's home or wherever they might be; use in smart cards; passports; and potentially most privacy invasive of all, actually inserted into the human body (Ball et al, 2006, 9.8).

Reflecting the growing use of RFID tags (it is estimated that in 2011 2.8 billion will be sold globally, a third of which will be in Europe), the European Commission has recently signed a voluntary agreement by which companies who sign up to the agreement commit themselves to carrying out a Privacy Risk Assessment (PIA) before they release the RFID product onto the marketplace. (European Commission Press Release, 2011). The Agreement establishes a specific Framework by which signatories will adhere in making their PIA. (European Commission, 2011). Included in the PIA, RFID operators must assess the risk of third parties being able to access personal data from the tags that come within the range of third party RFID readers. This was a particular concern where tags were used in the retail sector and were not deactivated when goods left the store. The recommendation allows a tag to remain active if the PIA concludes that the active tag does not represent a likely threat to privacy or the protection of personal data. The PIA is another example of privacy by design which has been advocated as an important element in the overall structure of providing effective privacy protection, but to date the primary focus has been on regulatory provision arguably (Article 29 Working Party, WP 180).



#### **4. The European Union regulatory structure for privacy protection**

When considering the regulatory structure for the protection of privacy provided by the European Union (EU), an appropriate starting point is the recognition that the EU has within its Charter of Fundamental Rights included two specific privacy related rights, Article 7 providing for respect for private and family life, which mirrors Article 8 of the European Convention on Human Rights, and Article 8 which provides for the protection of personal data.

With the coming into force of the Lisbon Treaty in 2009, not only has the Charter of Fundamental Rights become binding on most member states, but, additionally the Treaty of Rome, which established the European Community, was amended and renamed the Treaty on the Functioning of the European Union (TFEU); the renamed treaty includes Article 16, which replaces and expands upon the old Article 286, and it is hoped will give data protection within the EU new impetus. As the new legal basis for data protection in the EU, Article 16 is applicable to the processing of all personal data in the private and public sectors, including in the area of police and judicial co-operation and common foreign and security policy (Article 29 Working Party: WP168, 5-9).

In looking at profiling and especially profiling carried out where behavioural advertising is being undertaken, both Directive 95/46/EC (Data Protection Directive) and Directive 2002/58/EC (e-Privacy Directive), as amended by Directive 2009/136/EC, are applicable. Directive 95/46 provides protection for individuals in respect of the processing of their personal data. Key elements are the interpretation of processing, which is given a wide scope under the Directive and includes, for example, collection, recording, storage and alteration, and what constitutes personal data, with article 2 defining personal data as any information relating to an identified or identifiable natural person. It is important to appreciate that a broad notion of what personal data can be considered to be is provided for by the Directive (Article 29 Working Party, WP 136).

Recital 26 of the Directive provides important guidance on when a person might be considered identifiable from the information, stating, 'account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person,' and it continues, 'the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.' Thus, it would appear where data has been rendered anonymous so that an individual is no longer identifiable, and as well it is unlikely that the individual will be identified taking into account the means that are likely to be made reasonably by a data controller or third party, then the

data will not be considered personal data coming within the scope of the Directive's provisions. However, it is somewhat problematic to assess precisely what might be considered reasonably likely to happen, and each situation would need to be considered on its own facts. What is clear is that complete anonymisation of personal data in order to hide an individual's identity has been shown recently to be, if not a complete fallacy, then, certainly, not as secure or watertight as it was once considered to be in this regard (Ohm, 2010: 1716-1722). With the emergence of powerful re-identification algorithms it is argued that de-identification techniques designed to provide privacy protection are badly flawed (Narayanan & Shmatikov, 2010).

The e-Privacy Directive 2002/58 provides for the protection of privacy in respect of the processing of personal data in the electronic communications sector. Article 5 of the Directive seeks to ensure communications confidentiality by, for example, protecting against unauthorised listening, tapping or other forms of surveillance of communications over public communications networks or publicly available communications services. The recent amendment to Article 5(3) brings about a fundamental change in users privacy protection, in that the storing of information or the gaining of access to information already stored in the user or subscriber's terminal equipment will only be allowed with the user's prior consent, when they have been provided with clear and comprehensive information, in accordance with Directive 95/46/EC of the purposes for the processing. The change introduced means that rather than the user having to opt out to prevent the processing of their personal data across communications networks, they will now need to specifically opt-in to allow such processing. It needs to be pointed out that the Article 5 provision does not prevent any technical storage or access which is required for the sole purpose of carrying out or facilitating the transmission of a communication over a network. The Article 5(3) provision applies to cookies, as tracking cookies are considered information which is stored on a user's equipment and the cookies are accessed by advertising network providers when a user visits an advertising networks partner website (Article 29 Working Party: WP 171, 8). Thus, a user will now have to specifically approve the placing of cookies on to their machines.

The provisions of the amended e-Privacy Directive are required to be introduced into member states national law by the 25<sup>th</sup> May 2011. The changes brought about by the amended Article 5(3) appear from a UK perspective as somewhat problematic. At a time of substantial economic difficulties across Europe, there is a belief that the amended provision could act as a potential inhibitor of on-line economic activity, and as such would be unwelcome. A specific concern in respect of cookies is whether or not permission to place cookies on a user's machine would need to be obtained on every single occasion, and any consequential

impact on internet use and commercial activity that consequently might occur. The UK Government do however believe that consent will not be required in every situation, providing the example of where a cookie is essential for a service requested by the user, as with cookie use for a website shopping basket. (Vaizey 2011). This belief is based upon their interpretation of Recital 66 of Directive 2009/136/EC, which they consider via the use of browser settings allows consumers to indicate consent to cookies. Recital 66 states, 'Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user.' The Recital continues, 'Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application.' The UK government intends to directly copy the amended Article 5(3) into UK law, making reference as well to Recital 66. Work it is currently undertaking with browser manufacturers it is hoped will produce a browser setting solution that meets the consent requirement (Department for Culture, Media and Sport, 2011: 71-76). Doubts have, however, been raised over whether a browser based automatic consent mechanism will meet the Article 5(3) requirements, which the Article 29 Working Party consider is likely to happen in only very limited circumstances, as firstly, based upon the need for valid consent, a user cannot be deemed to have consented merely because they have used a browser which by default enables the collection of information. They argue, 'It is a fallacy to deem that on a general basis data subject inaction (he/she has not set the browser to refuse cookies) provides a clear and unambiguous indication of his/her wishes.' Secondly, they consider that for browser settings to be able to deliver informed consent, 'it should not be possible to "bypass" the choice made by the user in setting the browser'. This refers to the new generation of cookies that can be re-created after being deleted. Lastly, they consider that where the browser is set to receive cookies in bulk as a default, this implies that users are accepting processing without knowledge of the purposes or uses of the cookie, which in the circumstances cannot amount to valid consent (Article 29 Working Party: WP 171, 13-14).

As regards the information that is needed to be provided to users concerning the purposes of processing under Article 5(3), the UK government support Icon based initiatives that are currently being developed, by which a user can click on an Icon to receive details of the processing that will occur. (Vaizey, 2011), (Department for Culture, Media and Sport, 2011: 74). The Article 29 Working Party consider in respect of behavioural advertising that the use of Icons to facilitate information provision to the user is a positive move forward, and they

believe that the creation of a symbol with related messages would meet the need for consumers/users to be periodically reminded of the existence of targeted advertising taking place. (Article 29 Working Party: WP 171, 18). Whilst it is to be welcomed that the use of Icons in order to help with the provision of information to users is now being developed, it is regretful that it has taken so long for their potential usefulness to be recognised, as, indeed, I recommended their use in this context some 10 years ago (McKenna, 2001: 349).

Reflecting the growing concerns over the impact of online advertising, the European Parliament have recently adopted a resolution which in respect of behavioural advertising and its effect on personal privacy makes several specific requests to the European Commission, which call for action to be taken; these include developing educational material that explains how consumers can protect their privacy online, and requesting that the Commission as soon as possible require the insertion of the words 'behavioural advertisement' into online advertisements, with a window providing a basic explanation of behavioural advertising practice. A further interesting feature of the resolution comes in respect of hidden advertising. The Parliament condemns the developing online practice of the so-called hidden internet advertising, which occurs when comments posted on social network sites ostensibly by distinct autonomous individuals are in reality made as part of a co-ordinated campaign seeking to influence attitudes and behaviour. The Parliament is calling on the Commission to look at the Unfair Commercial Practices Directive (2005/29/EC) which relates solely to business and consumer relationships, to consider whether it needs updating to meet such new challenges. (European Parliament, 2010). Article 5 of the Directive provides 'A Commercial practice shall be unfair if..(b) it materially distorts or is likely to materially distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed..' Whether such manipulative behaviour can be considered to fall within the realm of privacy infringement is arguable, although such activities do seek to change behavioural patterns based upon potentially the interpretation of personal messages and information. Such manipulation in the online environment is not restricted to commercial operators, with it being recently reported that the United States military is developing software to manipulate social media sites by the creation of fake personas to influence internet discussions (Fielding & Cobain, 2011).

It is clear that the European Commission believe Europe's privacy laws still need updating further to meet new challenges faced in the digital age and as such proposals will be put forward this summer by the European Commission to update Directive 95/46. The EU Justice Commissioner Viviane Reding has recently provided some overarching guidance as to key areas of focus. In seeking to enhance the protection of an individual's personal data, she considers that the individual

rights should be built upon four pillars: (1) "The right to be forgotten" – in updating the rules in this regard to better protect online privacy, she is seeking to provide individuals the right, not just what she terms the "possibility", (reflecting difficulties that can be encountered), to withdraw their consent to data processing. (2) "Transparency". Reding argues, 'Individuals must be informed about which data is collected and for what purposes.' For her, individuals must know their rights, and all information concerning the protection of personal data must be given in a clear and intelligible way. (3) "Privacy by default". A key interpretation of this is an overarching requirement that consent must be obtained in all situations where personal data is collected. (4) "Protection regardless of location". It is proposed that no matter where in the world a service provider is located and the means they use to provide their service, homogenous privacy standards for European citizens should apply. Thus, any company that operates in the EU marketplace or in the online environment, and who targets EU citizens, would be expected to comply with EU privacy regulations (Reding, 2011). This would prove a significant change, as currently under Directive 95/46 non-EU based data controllers, who do not use equipment situated in the EU, fall outside its scope. (Article 29 Working Party, WP 168, page 9). It has already been questioned whether such a provision in reality is feasible, given its extra-territorial nature. (OUT-LAW, 2011).

## 5. Conclusion

With the reliance we now place on ICT's, never before in human history has it been so easy, as it is today, to collect and collate so much information about individual people, enabling sophisticated profiling to take place, and providing the potential for surreptitious manipulation of human behaviour on a mass scale to occur. Clearly, information and communications technologies will continue to be developed, becoming ever more sophisticated, and potentially privacy invasive. In looking to provide protection against the varied forms in which privacy infringement may be seen to occur, regulatory provisions arguably no matter how strongly constructed, are by themselves insufficient to provide an adequate level of protection. Whilst regulation can lay down the ground rules which are meant to be adhered to, the penalties to be faced where infringement is discovered, and act as an inhibitor to infringing behaviour, ultimately they cannot by themselves be a total safeguard. What is required is an holistic approach that in addition to a strong regulatory framework, includes as well protection via the notions of privacy by design, privacy enhancing technologies, self regulatory initiatives, information provision in a variety of formats with a prime example the development of Icon based information provision, and last but certainly not least, consideration as to how to utilise general educational provision to enable users to look to

protect themselves. However, what must be recognised is that even with such an holistic approach ultimately there is no full proof way of guaranteeing an individual's privacy, and never will be, and the best we can hope to achieve is to devise the strongest feasible protection strategy we can.

The concern raised in this paper is that with the collecting and profiling of personal information in whatever form, it may then be possible to use such data to manipulate human behaviour. This, if taking place without the knowledge of the targeted individual is a clear infringement of personal autonomy, and equally from a societal perspective a worrying development. It may be asked whether such manipulative technique usage should always be seen in a negative light however? There have been concerns recently in Europe over teenage suicide. In seeking to protect vulnerable teenagers, one potential approach utilising online digital technology could, for example, be based upon work carried out by a research team that looked at what information could be obtained by analysing keyboard typing patterns. The researchers believe that it is possible to identify when someone is under stress by using such analysis, and it could also be used to identify the onset of a condition, such as Alzheimers (Blincoe, 2010). If it were possible to identify a potential teenage suicide victim via such profiling or by using it in combination with other forms of profiling, would it then be unacceptable to attempt to use online manipulative behavioural psychology to try to change a teenager's immediate mood? Again, it must be argued that it comes down to the issue of personal autonomy of the individual and the need for there to be awareness of what is happening. For whilst in such a situation as this there may be a clear humanitarian concern, where do we draw the boundaries, and where do we stop?

## References

Angwin, J. and McGinty, T. (2010), Sites Feed Personal Details to New Tracking Industry, Wall Street Journal, 30<sup>th</sup> July 2010.

Article 29 Working Party, The Future of Privacy, WP 168, December 2009.

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP136, June 2007.

Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, WP 171, June 2010.

Article 29 Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180, 11<sup>th</sup> February 2011.

Ball, K., Lyon, D., Murakami Wood, D., Norris, C. and Raab, C. (2006), *A Report on the Surveillance Society*, Surveillance Studies Network.

Blincoe, R (2010), Your keyboard knows that it's you and you're stressed. *New Scientists* 7<sup>th</sup> January 2010. Online at [www.newscientist.com/article/dn18350-your-keyboard-knows-that-its-you-and-youre-stressed.html/](http://www.newscientist.com/article/dn18350-your-keyboard-knows-that-its-you-and-youre-stressed.html/) accessed 17.04.2011.

Burkert, H. (1999), *Privacy – Data Protection: A German/European Perspective*. Online at [www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf/](http://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf/) accessed 07.04.2011.

Cohan, N. (2011), *Its Tracking Your Every Move and You May Not Even Know*. *New York Times*, 26<sup>th</sup> March 2011.

Clifton, C., Mulligan, D. & Ramakrishnan, R (2006), *Data Mining and Privacy: An Overview*, in Strandburg, K and Stan Raicu, D (Eds), *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, Springer Science.

DARPA (2011), *DARPA Kicks off Mind's Eye Program*, January 4<sup>th</sup> 2011. Online at [www.darpa.mil/NewsEvents/Releases/2011/2011/01/04\\_DARPA\\_Kicks\\_Off\\_Mind's\\_Eye\\_Program.aspx/](http://www.darpa.mil/NewsEvents/Releases/2011/2011/01/04_DARPA_Kicks_Off_Mind's_Eye_Program.aspx/) accessed 13.04.2011.

Department for Culture, Media and Sport (UK), *Implementing the revised EU Electronic Communications Framework*, April 2011. Online at [www.culture.gov.uk/images/publications/FWR\\_implementation\\_Governmentresponse.pdf/](http://www.culture.gov.uk/images/publications/FWR_implementation_Governmentresponse.pdf/) accessed 17.04.2011.

European Commission (2011). *Privacy and Data Protection Impact Assessment Framework for RFID Applications*. 12.01.2011. Online at [ec.europa.eu/information\\_society/policy/rfid/documents/info-2011-00068.pdf](http://ec.europa.eu/information_society/policy/rfid/documents/info-2011-00068.pdf) accessed 13<sup>th</sup> April 2011

European Commission Press Release (2011). *Digital Agenda: new guidelines to address privacy concerns over use of smart tags*. IP/11/418. 06.04.2011.

European Parliament (2010). *Resolution of 15 December 2010 on the impact of advertising on consumer behaviour (2010/2052(INI))*.

Fielding, N. & Cobain, I. (2011), *Revealed: US spy operation that manipulates social media*, *The Guardian*, 17<sup>th</sup> March 2011.

Franco-British Council (2010), *How can France and the UK help citizens make better choices?* 17<sup>th</sup> November 2010. Online at [www.francobritishcouncil.org.uk/conferences.php?id=35/](http://www.francobritishcouncil.org.uk/conferences.php?id=35/) accessed 10.04.2011

Gutwirth, S. and De Hert, P. (2008), *Regulating Profiling in a Democratic Constitutional State*, in Hildebrandt, M and Gutwirth, S (Ed), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science.

Hildebrandt, M. (2008), Defining Profiling: A New Type of Knowledge?, in Hildebrandt, M and Gutwirth, S (Ed), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science.

Hill, S. (2011), There's No Sense Stressing About the End of Privacy. *E-Commerce Times*, 15<sup>th</sup> April 2011. Online at [www.ecommercetimes.com/story/72271.html?wlc=130293354/](http://www.ecommercetimes.com/story/72271.html?wlc=130293354/) accessed 16.04.2011.

Institute for Government (2010), *MINDSCAPE: Influencing behaviour through public policy*.

International Data Commissioners (2009), *Madrid Resolution: International Standards on the Protection of Personal Data and Privacy*, 6<sup>th</sup> November 2009. Online at [www.hldataprotection.com/uploads/file/madridresolutionnov09.pdf/](http://www.hldataprotection.com/uploads/file/madridresolutionnov09.pdf/) accessed 10.04.2011

Internet Advertising Bureau (2011), *Europe commits to self regulation*. 14<sup>th</sup> April 2011. Online at [www.iabuk.net/en/1/europecommittoselfregulation140411.mxs/](http://www.iabuk.net/en/1/europecommittoselfregulation140411.mxs/) accessed 16.04.2011.

Jarvis, J. (2011), *Revealed: US spy operation that manipulates social media*,

Keats Citron, D. (2010), *Mainstreaming Privacy Torts*, Cal. L. Rev, 98, 1805-1852.

Lessig, L. (1999), *Code and other laws of cyberspace*, Basic Books.

McKenna, A. (2001), *Playing Fair with Consumer Privacy in the global On-line Environment*, *Information & Communications Technology Law*, 3, 339-54.

Melville-Brown, A. (2008), *Camera shy – the interaction between the camera and the law of privacy in the UK*, *International Review of Law Computers & Technology*, Vol. 22, 3, 209-222.

Monmonier, M. (2006), *Geolocation and Locational Privacy: The “Inside” Story on Geospatial Tracking*, in Strandburg, K and Stan Raicu, D (Eds), *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, Springer Science.

Narayanan, A. & Shmatikov, V. (2010), *Privacy and Security: Myths and Fallacies of “Personally Identifiable Information”*. *Communications of the ACM* 53(6) June 2010.

O'Donnell, G. (2010), *Applying behavioural insight to health*, Cabinet Office, 31 December 2010. Online at [www.cabinetoffice.gov.uk/resource-library/applying-behavioural-insight-health/](http://www.cabinetoffice.gov.uk/resource-library/applying-behavioural-insight-health/) Accessed 10.04.2011.

Office of Fair Trading (2010), *Online Targeting of Advertising and Prices: A market study*, OFT131, May 2010.



Ohm, P. (2010), Broken Promises of Privacy: Responding to the Surprise Failure of Anonymization, 57 UCLA Law Review 1701-1777.

OUT-LAW News (2011), EU privacy law will extend to US social networks, vows Commissioner. 17th March 2011. Online at [www.out-law.com/page-11824-theme=print/](http://www.out-law.com/page-11824-theme=print/) accessed 17.04.2011.

Prime Minister's Strategy Unit (UK) (2004), Personal Responsibility and Changing Behaviour: the state of knowledge and its implications for public policy.

Prosser, W. (1960), Privacy, Cal. L. Rev, 48, 383-423.

Reding, V. (2011), Your data, your rights: Safeguarding your privacy in a connected Privacy Platform "The Review of the EU Data Protection Framework". 16<sup>th</sup> March 2011. Speech/11/183. Online at [europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183](http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183) accessed 03.04.2011.

Ross, J., Retail technology and the evolving shopper. Online at [www.shopper-sciences.com/storage/TheEvolvingShopper\\_v4\\_SHS.pdf/](http://www.shopper-sciences.com/storage/TheEvolvingShopper_v4_SHS.pdf/) accessed 12.04.2011.

Schermer, B. (2011), The limits of privacy in automated profiling and data mining, Computer Law & Security Review 27, 45-52.

Simitis, S. (2010), Privacy – An Endless Debate? Cal. L. Rev, 98, 1989-2005.

Soltani, A., Canty, S., Mayo, Q, Thomas, L & Hoofnagle, C (2009), Flash Cookies and Privacy. 10<sup>th</sup> August 2009. Online at [ssrn.com/abstract=1446862/](http://ssrn.com/abstract=1446862/) accessed 12<sup>th</sup> April 2011.

Tirtea, R., Castelluccia, C. and Ikonomidou, D. (2011), Bittersweet cookies: Some security and privacy considerations. ENISA, February 2011. Online at [www.enisa.europa.eu/act/it/library/pp/cookies/](http://www.enisa.europa.eu/act/it/library/pp/cookies/) accessed 10.04.2011.

Vaizey, E. – UK Minister for Culture, Communications and Creative Industries (2011), CBI forum on e-privacy and the digital economy – 29<sup>th</sup> March 2011. Online at [www.culture.gov.uk/news/ministers\\_speeches/7997.aspx/](http://www.culture.gov.uk/news/ministers_speeches/7997.aspx/) accessed 09.04.2011.

Van der Hof, S. and Prins, C. (2008), Personalisation and its Influence on Identities, Behaviour and Social Values, in Hildebrandt, M and Gutwirth, S (Eds), Profiling the European Citizen: Cross-Disciplinary Perspectives, Springer Science.

Warren S., and Brandeis, L. (1890), The Right to Privacy, Harv. L. Rev, 4, 193-220.

Zarsky, T. (2006), Online privacy, Tailoring, and Persuasion, in Strandburg, K. and Stan Raicu, D. (Eds), Privacy and Technologies of Identity: A Cross-Disciplinary Conversation, Springer Science.

# **The struggle over privacy, security, cyber-crimes and the civil rights in the Brazilian law – a historical overview**

---

---

**Rubens Menezes de Souza**

---

---

## **Introduction**

With one of the highest rates of Internet adoption in the world<sup>1</sup>, the Brazilian society is facing new challenges regarding regulation of the digital landscape. Questions related to privacy, cyber-crimes, data security and, most notably, intellectual property are emerging amongst tribunals, the media, social activists, scholars and politicians.

This paper will first focus on the current Brazilian legal landscape about this matters, presenting the consolidated legislation and the current tendencies adopted by its tribunals, also it will deal with many other ongoing reform propositions of the Brazilian laws that are focused on conflictive events that may occur over computer based interactions, especially the ones that take place on the Internet.

The reform propositions can only be understood exposing the actors who defend them, and they will be presented playing their roles as representatives of different interest groups on the struggle to adapt, change or, somehow, interfere in the Brazilian law. Then, with a clear understanding of who the actors are, it is possible to pinpoint the major debate forces, represented by the conservatives and the leftist-oriented intelligentsia.

Their methods of interference on the how public debates are carried out will be the main interest of this text, that is due to the fact that at the moment, very innovative propositions and experiences on the ways of how this debates are conducted, and on how the laws are written, are being tested in Brazil. Some of these debates are opened to the whole society, and even to foreigners (something that some people consider to be an aberration). Of course it remains to be proved if these processes are as open as they are portrayed and if they can survive to the traditional legislative process that will follow, especially if one took into consideration the debating parties large political spectrum, one heterogeneous cho-

---

1. GNETT-IBOPE/NetRatings (4th trimester/2008) in <http://www.cetic.br/usuarios/ibope/tab02-06.htm>.

rus of voices that has generated quite conflictive, contradictory and different law propositions.

Looking at how these debates have evolved, mostly in the last ten years with a historical criticism, makes it possible to grasp some perspective on how the different sides have been trying to win the hearts and minds of the civil society. Ultimately their actions, voices and reasoning captured and crystallized in these debates can lead to very interesting conclusions on if whether or not Brazil is fulfilling its largely advertised creation of new laws, and specially if the current civil rights can survive to this process.

### **A Brief overview on political history**

Brazilian law initially derives from the Portuguese Civil Law and has, over the years, acquired its own face. To understand the current Brazilian Civil Law it is necessary to consider a little bit the country's history that will be briefly presented in the next few paragraphs.

Brazil is the only Portuguese-speaking country of the Americas, and has began its history (in 1500 A.C.) as one of the many Portuguese colonies. It kept the colonial status until 1815 when, after being forced out off Europe by Napoleon, the Portuguese monarchy sought refuge in the new continent, arriving at Rio de Janeiro, and making the city the new capital (1808), instead of Lisbon<sup>2</sup>. Consequently Brazil became part of the "United Kingdom of Portugal, Brazil and Algarves"<sup>3</sup>, a status that made the country the first (and only) country of the Americas to ever become a monarchy, with a complete European royal family directly ruling over it. So the Brazilian law, has began – against all the odds – as a law systems founded in the monarchy system and rules.

But that was not a situation meant to last, once the independence from Portugal reached Brazil in 1822, first as one "independent" Brazilian Empire, ruled by the son of the original king; afterwards, in 1824 Brazil had its first Constitution ratified, implementing a bicameral legislature, that latter was be the Congress and, finally, in 1889, it would become a Republic.

Historians name the period from 1889 to 1930 as Old Republic (República Velha in Portuguese), a period where Brazil would call itself a Democratic Republic, but would hardly meet the minimum requirements to be named that way, considering that, just as an example, no woman could vote. The power would be, in

---

2. István Jancsó, org., *Cronologia de História do Brasil Colonial (1500-1831)*, Série Iniciação 1 (São Paulo: FFLCH-USP, 1994), 192.

3. Ibidem, 206.

fact, shared between the oligarchies of the two richest states of the union: São Paulo and Minas Gerais. The 1929 world crisis and its effect over Brazilian agricultural economy produced the necessary crisis amongst the established powers, and brought new forces in the political arena. The Old Republic period ended in 1930 with the rise of President Getúlio Vargas, a civilian dictator from the southern state of Rio Grande do Sul, installed by a military *coup d'état*, marking both the end of Old Republic and the beginning of the "Vargas Era".

It might seem odd to see a country decaying from a Democratic Republic to a Dictatorship political system. However it is interesting to note that neither democracy nor republicanism, were universal values for the people at this period. All efforts to make ideological approximations with the French or North-American democratic values were just nominal and made by the oligarchies when justifying their own domination over the State. In 1930 Vargas promoted the dissolution of Congress, the abrogation of the country's 1891 Constitution and put an end to the dominance cycle of São Paulo and Minas Gerais oligarchies. Around 1930 Brazil was a very different country, living the infancy of its industrialization that saw a first minor burst from 1880-1890<sup>4</sup>, when the country was still transitioning from the slave work forces to wage working forces, a necessary step towards industrialization. This is also the time when Brazil, and Latin America in general, had their major urbanization jumping from a 37,7 per cent of the population living in urban areas in 1940 to 69,4 per cent in 1980<sup>5</sup>.

President Vargas ruled Brazil as dictator until 1945, when he was forced out of the office by another *coup d'état*. His dictatorship was marked by strong fascist-influence and persecution of leftist-oriented parties, namely, the communists that had tried insurrection in 1935, heavily squashed and then used as decades long propaganda against communists and left-oriented parties<sup>6</sup>. The period that starts in 1946 is remembered by its great political instability and was named Second Republic by the historians. President Vargas, who maintained strong influence during the Second Republic, returned from 1951 to 1954 as an elected President; after that he committed suicide, putting an end to the Vargas Era.

---

4. Sergio Silva, *Expansão Cafeeira e Origens da Indústria no Brasil* (São Paulo: Alfa-Omega, 1976), 80.

5. Orlandina de Oliveira e Bryan Roberts, "O Crescimento Urbano e a Estrutura Social Urbana na América Latina, 1930-1990", in *História da América Latina: a América Latina após 1930: Economia e Sociedade*, vol. VI (São Paulo: Edusp, 2005), 302-303.

6. Daniel Aarão Reis, "Entre Reforma e Revolução a Trajetória do Partido Comunista no Brasil entre 1943 e 1964", in *História do Marxismo no Brasil - Partidos e organizações dos anos 1920 aos 1960*, vol. 5 (Campinas: Editora da UNICAMP, 2007), 73.

The political instability that followed this period led to the infamous 1964 *coup d'état* that would keep Brazil under an authoritarian military government from 1964 to 1985, again a period of great persecution of the left aligned parties and ideologies.

In 1985 the civilian José Sarney<sup>7</sup>, a politician from Maranhão, a northern Brazilian state, was finally named President. That happened after Tancredo Neves<sup>8</sup>, a politician of southern state Minas Gerais, who was appointed President by the congress, died of natural causes before assuming the presidency office. Today, as defined by the 1988 Constitution, Brazil is a Federal Republic that congregates 26 states, the Federal District, and over five thousand municipalities.

After the promulgation of the 1988 Constitution, Brazil held a direct democratic election, in 1989 – the first in almost 30 years – bringing Fernando Collor de Mello<sup>9</sup>, a politician, born in Rio de Janeiro, but based in the northeastern state of Alagoas, to the presidency office. President Collor was elected with an agenda that focused in combating the corruption of José Sarney's years and concluding the transition to a civilian government after the “plumb years<sup>10</sup>” of military rule. President Collor also began the process of opening, i.e. liberalizing, the Brazilian markets, an aspect of the economic life that the military has kept under tight control, especially in the areas considered strategic such as computing<sup>11</sup>.

After being accused of an enormous corruption in 1991, President Collor started to face protests all over the country, and was driven to resignation in 1992. His resignation was a maneuver to avoid the Senate voting for his impeachment, something that happened anyway, and suspended his political rights for the following eight years, under Brazilian law<sup>12</sup>.

7. “José Ribamar Ferreira de Araújo Costa - José Sarney — Presidência da República Federativa do Brasil”, [s.d.], [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/galsarney](http://www.presidencia.gov.br/info_historicas/galeria_pres/galsarney).

8. “Tancredo de Almeida Neves — Presidência da República Federativa do Brasil”, [s.d.], [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/galtancredo](http://www.presidencia.gov.br/info_historicas/galeria_pres/galtancredo).

9. “Fernando Afonso Collor de Mello — Presidência da República Federativa do Brasil”, [s.d.], [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/galcollor](http://www.presidencia.gov.br/info_historicas/galeria_pres/galcollor).

10. Brazilians often refers to the military years after the 1964 *coup d'état* as “anos de chumbo” or “plumb years” in English.

11. Ivan da Costa Marques, “Cloning Computers: From Rights of Possession to Rights of Creation”, *Science as Culture* 14 (2) (junho 2005): 139-160.

12. As a side note, it is interesting to mention that Collor, the first Brazilian elected President after the military regimen, and also first impeached President ever, has won the second term of the 1989 election against Lula, who would be elected the President latter in 2002. Today, in 2011, Collor is one elected senator by the northeast Alagoas state, his political base.

After Collor's impeachment Itamar Franco<sup>13</sup>, his vice president and a Minas Gerais state politician, assumed the presidency for the remainder term. President Itamar faced a major economic crisis and stratospheric inflation rates, reaching over a 1000 (thousand) per cent a year in 2003. He named Fernando Henrique Cardoso (also known as FHC), a São Paulo state politician, the Minister of Treasury. After decades of close to desperation attempts of controlling the inflation – where Presidents Sarney and Collor both had failed – FHC managed to get the inflation under control with his Plano Real, that established a new currency in Brazil. This major accomplishment made it possible for FHC to be elected in the 1994<sup>14</sup> in the presidential run, and even re-elected in 1998<sup>15</sup>.

In 2002, Luiz Inácio “Lula” da Silva<sup>16</sup>, of the leftist Workers Party, the well-known PT, finally got elected as president, after being defeated by President Fernando Collor de Mello in 1989, and President Fernando Henrique Cardoso in 1994 and in 1998. Lula's election marked one notable turn in Brazilian politics, once for the first time a leftist-oriented party won a democratic election in Brazil, an important political factor for the arguments that are going to be discussed in this paper in the following pages, and to better illustrate many conflicts that would happen later on. President Lula served for two terms<sup>17</sup>, and in October of 2010, Dilma Rousseff<sup>18</sup>, from the same Workers Party (named PT), got elected to Brazil's presidency, being the first woman ever to realize such an achievement in Brazilian politics. To understand the genesis of these conflicts it is necessary to explain how PT has become the major left aligned party in Brazil.

PT was officially founded in 1980, as a reflex of the new classes emerging from the industrialization and also from the growth of the urbanization. Paulo Hen-

---

13. “Itamar Augusto Cautiero Franco — Presidência da República Federativa do Brasil”, [s.d.], [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/galitamar](http://www.presidencia.gov.br/info_historicas/galeria_pres/galitamar).

14. “Fernando Henrique Cardoso — Presidência da República Federativa do Brasil”, [s.d.], [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/galfhc1](http://www.presidencia.gov.br/info_historicas/galeria_pres/galfhc1).

15. “Fernando Henrique Cardoso (2) — Presidência da República Federativa do Brasil”, [s.d.], [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/galfhc](http://www.presidencia.gov.br/info_historicas/galeria_pres/galfhc).

16. “Luiz Inácio Lula da Silva — Presidência da República Federativa do Brasil”, [s.d.], [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/Lula](http://www.presidencia.gov.br/info_historicas/galeria_pres/Lula).

17. “Luiz Inácio Lula da Silva (2) — Presidência da República Federativa do Brasil”, [s.d.], [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/Lula2](http://www.presidencia.gov.br/info_historicas/galeria_pres/Lula2).

18. “Dilma Rousseff — Presidência da República Federativa do Brasil”, [s.d.], [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/dilma-rousseff](http://www.presidencia.gov.br/info_historicas/galeria_pres/dilma-rousseff).

rique Martinez<sup>19</sup> traces the origins of PT back to the middle 60's, and he describes the social groups that got together in the party as follows:

*"The social bases that constituted PT were composed mainly of industrial workers, such as metallurgical, chemical, oil, leather, and glass workers; service sector workers like employees of transport companies, banks, small capitalists and landless rural workers, also civil servants such as teachers of municipal and state schools.*

*The composition of this social base also aggregated numerous politically radicalized segments of the middle classes, bound by work and also by participation in different organized social movements, mostly urban, like the ones for housing, better wages, jobs, education and health. (...) The connection with the world of work, predominantly the waged work, assured the social identity that shaped and named the new party: of the Workers"*<sup>20</sup>

If until 2002 the power balance in Brazil would be changing amongst different representatives of the same dominant elite, swinging between the more and the less conservative, with the victory of PT in 2002 elections, a different group would arrive to power, making room, if not for changes, at least for possibility of changes.

It is still an open debate if PT has, from its foundations in 1980 to the election of 2002, kept itself faithful to the original propositions or even to the original segments that helped in its creation, but there is no doubt that, in many aspects, after 2002 the political agenda in Brazil was opened to incorporate new practices and new propositions, leading to the first major movements to propose relaxation of copyright laws and also some kind of Internet regulation that would primarily reassure fundamental rights to citizens in place of trying to control or coerce their on-line activities.

### **The Brazilian laws on privacy, security, crimes and intellectual property**

Since Brazilian law was at first inherited from Portugal, it is natural to assume that it had preserved some of its characteristics like being hierarchically organized. This means that the states got their individual judiciary systems, but all of them are limited by the federal judiciary. The system is mirrored on the Roman-Germanic tradition, based on statutes and law, but since a 2004 Constitutional

---

19. Paulo Henrique Martinez, "O Partido dos Trabalhadores e a Conquista do Estado 1980-2005", in *História do Marxismo no Brasil - Partidos e movimentos após os anos 1960*, vol. 6, 6 vols. (Campinas: Editora da UNICAMP, 2007), 464.

20. PT stands for Partido dos Trabalhadores, that translates as Workers Party.

Amendment, was introduced the *Súmula Vinculante*, a mechanism similar to *Stare Decisis*, so there could be more uniformity on decisions made by the judiciary, the *Súmula Vinculante* can be stated only by the Supreme Court of Brazil.

The Constitution rules above all the other laws, and no law can dictate against it, or it will be held unconstitutional and, theoretically, annulled. By constitutional determination Brazilian citizens have granted rights to free speech and thought, but no right to anonymity, which is, in fact, prohibited by the Constitution.

A brief look at the constitutional rights of the Brazilians, in the Constitution of 1988, is enough to imagine the great judiciary mess that would be installed ten years latter, with the wide spread use of the Internet in the country.

In the Title II <sup>21</sup>, devoted to “*Fundamental Rights and Guarantees*”, Chapter I is where Constitution defines the Rights and Duties of Groups and Individuals. Art. 5<sup>th</sup>, Item IV <sup>22</sup> clearly states: “*The manifestation of thinking is free, but anonymity is forbidden*”, the reasoning of the legislators is plain obvious when we read Art. 5<sup>th</sup>, Item V assuring the right of answer, and material reparation in cases of material, moral or image damages. The concept is that Brazilians are free to say whatever they want, but responsibility should be attached to it, and, therefore, consequences.

Art. 5<sup>th</sup>, Item IX deals with the right of free expression, and intellectual, artistic, scientific and communication freedoms, that should not face any kind of censorship or licensing interferences, and Art. 5<sup>th</sup>, Item X made it inviolable intimacy, private life, honor and image of the person, again, re-assuring possibility of compensation for material or moral damages if violations occur.

On correspondence, communications over phone, telegraphic or data communications, Art. 5<sup>th</sup>, Item XII made them inviolable, in a way secrecy can only be broke by a judicial order intended to proceed criminal investigations, and only according with cases established by the law nº 9.296 of 1996. Even in this case there are clear limits to how far the state can dig in the course of investigations, we will get back to that latter. It is also important to note, that while anonymity is forbidden, Item XIV, grants to all access to information and allows confidentiality of sources.

The Brazilian Constitution of 1988, nicknamed Citizen Constitution, will also specifically regulate intellectual property rights, beginning in Item XXVII that re-

---

21. TÍTULO II: Dos Direitos e Garantias Fundamentais ; CAPÍTULO I: DOS DIREITOS E DEVERES INDIVIDUAIS E COLETIVOS.

22. Constituição da República Federativa do Brasil de 1988, Constituição da República Federativa do Brasil de 1988, [http://www.planalto.gov.br/ccivil\\_03/constituicao/constitui%C3%A7ao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm).



assures authors and their heirs' rights, providing that a specific law will determine the length of time for this protection, and continuing with Item XXVIII that will provide in even more details for authors' rights. Item XXIX regulates industrial innovations, the rights of the creators, and also, property over trademarks, companies names and other distinctive signs.

Other constitutional articles relevant to the purposes of this paper are the ones ranging from Items XXXIX to XLII, that will define the following principles:

XXXIX – there shall be no crime without prior law that defines it, neither punishment without previous legal sanction;

XL – the law shall never be retroactive, except in benefit of the defendant;

XLI – the law shall punish any act of discrimination against fundamental rights and freedoms;

XLII – the practice of racism shall be a crime unbailable and imprescriptible, subject to imprisonment under the law;

Many aspects of the Brazilian Constitution are defined only by their principles, needing a latter formulated law to define exactly on what grounds they will be applied. The above law 9.296/96 defines how Art. 5<sup>th</sup>, Item XII, dealing with communications, is implemented. The main highlights of this law will be scrutinized in the next paragraphs.

Before violating a person's communications secrecy it is mandatory to have one order from a competent judge and this law is valid to "interception of communications flow in informatics and telematics systems", which pretty much covers the Internet even in the most narrowed interpretations.

The 9.296/96 law also defines, (Art. 2<sup>nd</sup>), that the interception of communications will not be admitted when "there are no reasonable evidence of authorship or participation in penal infraction" and "evidence could be generated by other means available". It also states that the object of the investigation must be stated with precision and that monitoring should not exceed 15 days, renewable by the same period. Art. 7<sup>th</sup> of the same law opens the possibility for law enforcement to request specialized technical assistance of services operators, Art. 9<sup>th</sup> determines that "The recordings that do not relate to the sought evidence will be destructed by judicial determination, during the process, evidence gathering or after that, by the means of a request of the Ministério Público<sup>23</sup> or by the interested part.", also Ministério Público will witness the destruction, being optional the presence of defendant or its legal representative. Finally the 10<sup>th</sup> article of the 9.296/96

---

23. The independent Public Prosecutors.

law define as a crime to intercept communications if not in accordance with this regulations and, determines the punishment as “two to four years of reclusion, and a fine”.

So secrecy of electronic communications is a constitutional right in Brazil, and it also is resulated by a special statate, bringing strong principles and heavy punishments.

In relation to free speech and thinking, Brazilians are also well covered by their constitutional rights, even considering that they are not allowed to act anonymously when manifesting their ideas. We will return to this ideas latter when we compare them against the reality of courts and the new laws being proposed. Focusing on intellectual property rights, we have already seen that they are also granted by the Constitution, again, details of these rights and how they are implemented, are defined by specific laws.

### Long lasting rights...

The first Brazilian law to deal with immaterial property is the law nº 496/1898 in the 1830 Penal Code, until that point the authors rights in Brazil was, to quote Prof. Paranaçuá<sup>24</sup>, a “no man’s land”. Brazilian society interest for the protection, or mercantile fruition, of intellectual goods – as one would expect – was born and grew along the years the country made its transition to a capitalist economy and initiated its urbanization and industrialization.

In September 1886 Brazil adheres to the Berne Convention for the Protection of Literary and Artistic Works, initiating its relationship with international laws about immaterial goods. Also the 1891 Constitution<sup>25</sup> would, briefly, address intellectual property rights referring to a specific law for duration of the protections.

The 1916, the Civil Code revoked that original law and substituted it by articles nº 649 to nº 673 that dealt with “*Literary, Scientific and Artistic Property*”<sup>26</sup>. The 1898 law indicated that the length of time an authors’ work would be protected was for 50 years, counting from 1<sup>st</sup> of January of the year of publishing<sup>27</sup>;

---

24. Pedro Paranaçuá e Sérgio Branco, *Direitos Autorais*, 1st ed., FGV Jurídica (Rio de Janeiro: Editora FGV, 2009).

25. “Constituição da República dos Estados Unidos do Brasil de 1891”, [s.d.], [http://www.planalto.gov.br/ccivil\\_03/constituicao/Constitui%C3%A7ao91.htm](http://www.planalto.gov.br/ccivil_03/constituicao/Constitui%C3%A7ao91.htm).

26. Da propriedade literária, científica e artística.

27. Lei nº 496, de 1ª de agosto de 1898., Collecção das Leis da Republica dos Estados Unidos do Brazil de 1898, vol. I, 1898, <http://www2.camara.gov.br/legin/fed/lei/1824-1899/lei-496-1-agosto-1898-540039-publicacao-39820-pl.html>.

The 1916 Civil Code extended it to 60 years, counting from the day of author's death<sup>28</sup>. Ten additional years of protection in only 18 years time, and also already ten years beyond the time stipulated by Berne Convention.

It was only in 1973 that Brazil would enjoy a comprehensive and unified law regulating authors rights, law nº 5.988<sup>29</sup> made a minor adjustment to the length of protection, now being 60 years counting from 1<sup>st</sup> of January of the year after the author's death. This law was latter substituted by law nº 9.610<sup>30</sup> from 1998, the current Brazilian law for authors rights, where there was another change, providing additional ten years of protection in relation to 1973 law. Art. 41 determines:

"The author's economic rights endure for seventy years as of January 1 of the year following his death, obeying the order of succession under civil law"<sup>31</sup>

In Brazilian society, there has been a movement to extend property rights in favor of the authors in particular and to the detriment of society in general.

It is an interesting coincidence that this extension was made in the same year the North-American Congress approved the Sonny Bono Copyright Term Extension Act<sup>32</sup>. It is tempting to speculate about direct relationships between the two extensions, envisioning maybe, some kind of political pressure but in reality at this point in time, pressure for more strict and hard enforcement of intellectual property is scattered all over the globe.

The most complete example of this was the Trips Agreement, or Agreement on Trade-Related Aspects of Intellectual Property Rights<sup>33</sup>, that was in negotiation from 1986 to 1994, and basically introduced the Intellectual Property<sup>34</sup> in the WTO<sup>35</sup>.

---

28. Clovis Bevilacqua e Aquiles Bevilacqua, *Codigo Civil Dos Estados Unidos Do Brasil Commentado*, vol. 3, 9th ed. (Rio de Janeiro: Francisco Alves, 1916).

29. Lei nº 5.988, de 14 de Dezembro de 1973., 1973, <http://www.planalto.gov.br/ccivil/leis/L5988impressao.htm>.

30. Lei nº 9.610, de 19 de Fevereiro de 1998., 1998, <http://www.planalto.gov.br/ccivil/leis/L9610.htm>.

31. Art. 41. Os direitos patrimoniais do autor perduram por setenta anos contados de 1º de janeiro do ano subsequente ao de seu falecimento, obedecida a ordem sucessória da lei civil.

32. Sonny Bono, *Sonny Bono Copyright Term Extension Act*, 1998, [www.copyright.gov/legislation/s505.pdf](http://www.copyright.gov/legislation/s505.pdf).

33. *Trade-Related Aspects of Intellectual Property Rights*, 1994, [http://www.wto.org/english/docs\\_e/legal\\_e/27-trips\\_01\\_e.htm](http://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm).

34. Maristela Basso, "O Regime Internacional de Proteção da Propriedade Intelectual da OMC/TRIPS", in *OMC e Comércio Internacional*, org. Alberto do Amaral Júnior (São Paulo: Aduaneiras, 2006), 360.

35. World Trade Organization.

It is important to make two points about these ideas. First that from the two world-wide systems used to deal with authors' rights, Brazil is historically affiliated with the French idea of *droit d'auteur* and not with the British *copyright*<sup>36</sup>. Second, the doctrine dealing with the authors' rights understands these rights as fair, but that they should be limited in time, to the benefit of the whole society at some point. Concepts in contradiction with Brazilian position as the fourth worst-rated country by Consumers International IP Watchlist in 2011<sup>37</sup>.

The lack of flexibility, extended duration and criminalization of activities related to the reproduction of copyrighted materials in Brazil triggered the government initiatives to reform of the 9.610/98 law<sup>38</sup>. This reform, for the most of it, aimed to put in place regulations to assure the fair use of copyrighted materials, introducing some flexibility in a very strict law, promoting radical conceptions as the one that makes it illegal to place DRM, Digital Rights Management<sup>39</sup> technology, on works that have entered the public domain. This legal reform is quite unpopular amongst the copyright industry representatives in Brazil and abroad<sup>40</sup>.

## The civil landmark

Three major law reform propositions are now being discussed in Brazil. Those are: the Marco Civil da Internet<sup>41</sup> (Internet's Civil Landmark), a new LDA<sup>42</sup> (a New Copyright Law), and one Law about Personal Data Protection<sup>43</sup>. This paper focus on the first two, since the third one is still being debated within society as we write, also it would drive us far away from the legislation presented until now.

---

36. Paranaguá e Branco, *Direitos Autorais*.

37. Consumers International, *Consumers International IP Watchlist 2011* (Consumers International, 2011), <http://A2Knetwork.org>.

38. "Gilberto Gil: 'Pirataria é desobediência civil' - Terra - Cultura", março 5, 2009, <http://terramagazine.terra.com.br/interna/0,,OI3605448-EI6581,00-Gilberto+Gil+Pirataria+e+d+esobediencia+civil.html>.

39. Georg Erber, "Proprietary Digital Rights Management Systems and Music-Downloads - Obstacles for Innovation from a Competition Policy Perspective", *SSRN eLibrary* (setembro 18, 2009), [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1475059](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1475059).

40. "Quem tem medo da mudança?", *Link - Estadão.com.br*, março 20, 2011, <http://blogs.estadao.com.br/link/quem-tem-medo-da-mudanca/>.

41. "Marco Civil", [s.d.], <http://culturadigital.br/marcocivil/sobre/>.

42. "Consulta Direito Autoral", [s.d.], <http://www.cultura.gov.br/consultadireitoautoraleconsulta/>.

43. "Debate Público Proteção de Dados Pessoais", [s.d.], <http://culturadigital.br/dadospessoais/apresentacao-2/>.

When it was launched back in 2009, the very idea of Marco Civil was a radical change in how law and politics could be conducted by a government. Marco Civil is not a law, but a law proposition, formulated outside the legislative houses of the Brazilian Congress. The idea was to obtain a draft of the bill made by society, prior the necessary step of sending it to be voted and negotiated by congressman. The most radical concept was to use the Internet itself to formulate a law meant to regulate the Internet, in an extreme democratic approach the debate would be opened to everyone, including non-nationals of Brazil:

“The proposed construction of the regulatory framework also seeks to innovate the process of its formulation: the intent is to encourage, through the Internet itself, the objective and active participation of numerous actors involved in the debate (users, academics, representatives of private enterprises, parliamentarians and government representatives). For this, the process will be conducted primarily via the Internet itself.”<sup>44</sup>

This idea would latter be adopted by the Brazilian government to start other relevant discussions such as the ongoing revision the Copyright Law<sup>45</sup> and the formulation of a Personal Data Protection Law<sup>46</sup>.

At the moment (April, 2011) the debate is over and the final text, that can be found on-line<sup>47</sup>, is waiting to be presented to the Congress. Marco Civil was constructed as a very progressive bill but, during the text formulation, groups of Brazilian activists pointed out a possible interpretation of the new law that, as an unintended consequence, could drive to a forced monitoring, or registering requisite, to the Internet in Brazil, one possibility that would jeopardize civil liberties and, above all would be unconstitutional.

Marco Civil does not make this proposition directly. The problem resides in the crossing of different sentences along the proposed text, such as the suggestion for keeping access logs during a given period of time.

Many known free-speech, free-culture and free-software activists had manifested their discontentment with this idea<sup>48</sup>, even though, in principle, they support

---

44. “Marco Civil”. As above.

45. “Consulta Direito Autoral”, [s.d.], <http://www.cultura.gov.br/consultadireitoautoral/consulta/>.

46. “Debate Público Proteção de Dados Pessoais”, [s.d.], <http://culturadigital.br/dadospessoais/apresentacao-2/>.

47. “Marco Civil”. As above.

48. This feeling was pretty much materialized in their Twitter feeds and in the re-tweets of the protest messages. Some of them can be found (in Portuguese) at this addresses: <http://twitter>.

Marco Civil. The majority of the criticism pointed to a perception that keeping access logs would end up in a kind of compulsory registration to access Internet in Brazil.

### **Some propositions of Marco Civil are:**

Art. 2<sup>nd</sup>, that reassures freedoms and rights granted to the Internet user, including rights to privacy and free-speech.

Art. 4<sup>th</sup> paragraph VI establishes what are “logs of access to the Internet” and defining them as “the collection of information regarding the date and time of use of a particular Internet service from a particular IP number”, that is the definition of access logs from a technical point of view.

Chapter II, Art. 7<sup>th</sup> establishes users rights. Paragraph I grants “the inviolability and secrecy of communications, except by court order, in cases and in the manner provided by law for purposes of criminal investigation or criminal proceedings;” Paragraph IV extends the users rights assuring the “non-disclosure or use of the connection logs and records of access to Internet services, except upon the consent or due to court order”. Art. 8<sup>th</sup> continues assuring to the Internet users privacy, free-speech and granting the right to take personal measures to pursue this goals, something we believe is specifically mentioned in the proposition to legally grant citizens liberty to use proxy and encryption technologies.

It is in Chapter III, Art. 9<sup>th</sup> that the contradictions start to emerge when the proposition “imposes the obligation to keep connection records, according to Subsection I of Section III of this Chapter, being prohibited the keeping of access records of Internet services by the ISP”, and in Art. 14<sup>th</sup> defining that “The provision of Internet connection requires the administrator of the autonomous system corresponding duty to keep confidential records of connection in a controlled environment and security, for a maximum of 6 (six) months, in accordance with the regulation”

Art. 15<sup>th</sup> will deals specifically with the “*keeping of connection records*” this way:

*I - the connection logs can only be provided to third parties by court order or with prior written permission of the respective user;*

*II - the registration can only be available linked to connection logs by court order, and*

---

com/samadeu/status/12949772543, <http://twitter.com/samadeu/status/12950057728>,  
<http://twitter.com/MarceloBranco/status/13392755675> and <http://twitter.com/samadeu/statuses/13384481632>.

*III - the measures and procedures of security and confidentiality of records and registration data connection should be clearly informed to the users.” and “The security procedures necessary to preserve confidentiality and integrity of connection logs and registry data of this article must meet the appropriate standards to be set by specific regulation.”*

This proposition about logs becomes confusing and contradictory on the light of the above Art. 7<sup>th</sup> where “(...) except by court order, in cases and in the manner provided by law for purposes of criminal investigation or criminal proceedings;” and also with Paragraph IV “(...), except upon the consent or due to court order”

The point is that if “connection logs and access logs” exists stored at any place, like it is mentioned in Paragraph IV of Art. 7<sup>th</sup>, and considering that Art. 15<sup>th</sup>, Paragraph II makes it possible to cross connection data with registration data, it means that the value of privacy is being severely undermined. This situation is aggravated in Art. 15<sup>th</sup> when it does not clearly defines how this data is supposed to be kept, referencing “appropriate standards to be set” by nonexistent “specific regulation”.

Subsection II, explores “The Internet services access record keeping” where Art. 16<sup>th</sup> presents this text:

“The keeping of access records of Internet services depends on the user’s permission and must meet the following, without prejudice to other rules and guidelines relating to protection of personal data:

I - informing user about the nature, purpose, period of storage, security policies and destination of saved information by giving it access, possibility to correct and update the data whenever requested;

II - free and informed consent for the user prior to processing, distribution to third parties or publication of information collected, and

III - data allowing user identification can only be provided in a manner linked to access records of Internet services by a court order.”

The Problem is that the user consent, while pretty well defined by the proposed law, is innocuous once the court can request the already stored logs and registration data.

In any case scenario the fact that remains true is that whenever registration data (essentially name and billing address) and connexion data (IP address, time of access and addresses visited) exists stored, there is a possibility to rebuild and trace a user whereabouts on line with a simple computer query. This scenario can easily be interpreted as a form of compulsory registration to access the Internet, extinguishing in this way the anonymity of users.

### Who makes the laws?

Before proceeding with the criticism of Marco Civil it is important to understand the origin of this law proposition, why it was designed in public, and who are the political actors pushing it forward. At this point reconnecting the text with the historical and political panorama traced at the beginning is necessary.

During the 20<sup>th</sup> century, in Latin America established political parties and oligarchies saw the erosion of a significant parcel of its political power, mainly as a consequence for the expansion of urban areas.

“The industrial growth stimulated the elevation of education, proletarianization of workforce and also expansion of non-manual workforce. On the other side, this very urban growth brought with it one sharp polarization of the social structure, in terms of income and in terms of working conditions, (...) and a very distorted income distribution”<sup>49</sup>.

Brazil was no stranger to this movement where, slowly, rural oligarchies started to loose ground. In 2002 Lula finally got elected president, allowing his party, PT, to expand some policies first implemented in states and municipalities to a federal level.

There is no space here to explore the alleged differences, or to evaluate PT policies, nor that is the objective of this text, but there is one characteristic, common to almost all PT administrations, that probably reflected with great vivacity over the new method of laws formulations, created with Marco Civil: both the mentality and commitment with Open Source Software (OSS).

Since the first municipalities where PT managed to elect mayors, there has been a commitment from the party to explore the possibilities of implementation of Open Source Software in public administration and in digital inclusion of population.

“Porto Alegre, a southern Brazilian city is a metropolis with over 3 million people, during 15 years it had an unique experience when we consider the peculiarities of Brazilian politics. From 1989, during four successive administrations, until 2004, the Workers Party (PT) ruled the city, introducing innovations such as participatory budgeting, supporting the creation of the World

---

49. Oliveira e Roberts, “O Crescimento Urbano e a Estrutura Social Urbana na América Latina, 1930-1990”.



Social Forum<sup>50</sup> and becoming a center for the debate on the possibilities for the left in local scale changes.”<sup>51</sup>

Also it is in Porto Alegre, that for over eleven years, the FISL (International Forum of Free Software) takes place, sometimes at the same time as editions of the World Social Forum. This way, for almost two decades Porto Alegre has been – even when not under a PT administration – the lighthouse for free software advocates in Brazil. FISL helped to form a generation of leftist-oriented technicians, and expanded the OSS way of think to academics, lawyers and NGOs.

When in 2002 PT entered the federal administration, the culture of OSS was already deeply rooted into the party, where it got mixed with a discourse of technological independence and gained adepts out of technical circles, this led to the urge to implement Free Open Source Software all over the federal level, an initiative driven mostly by PT members from the cities of Porto Alegre and São Paulo, whom in less then eight years made Brazil an international reference in implementation of OSS<sup>52</sup>.

At almost the same time, the Minas Gerais state senator Eduardo Azeredo (from PSDB) become the major sponsor of a bill presented in 1999<sup>53</sup>, called by its detractors as “Digital AI-5”<sup>54</sup>, this bill intends to deal with “crimes committed in the area of informatics, its penalties and other measures” focusing in “virtual computer crimes or the attacks perpetrated by hackers and crackers”<sup>55</sup>. It is easy to see why this 84/1999 Law Project (or PL in Portuguese) meet instant hostility from PT technical militants, that in general can get offended by the mixed misuse of the words hacker and cracker<sup>56</sup>.

---

50. Created in opposition of the World Economic Forum. For more informations visit: [http://www.forumsocialmundial.org.br/main.php?id\\_menu=19&cd\\_language=2](http://www.forumsocialmundial.org.br/main.php?id_menu=19&cd_language=2).

51. “A esquerda no poder local: Porto Alegre e o Partido dos Trabalhadores”, September 12, 2009, <http://www.ub.es/geocrit/sn/sn-24516.htm>.

52. Todd Benson, “Brazil - Free Software's Biggest and Best Friend”, *Imprensa, NYTimes.com*, março 29, 2005, [http://select.nytimes.com/gst/abstract.html?res=F40614FD395B0C7A8EDDAA0894DD404482&fta=y&incamp=archive:article\\_related](http://select.nytimes.com/gst/abstract.html?res=F40614FD395B0C7A8EDDAA0894DD404482&fta=y&incamp=archive:article_related).

53. “PL-84/1999”, fevereiro 24, 1999, [http://www.camara.gov.br/sileg/prop\\_detalhe.asp?id=15028](http://www.camara.gov.br/sileg/prop_detalhe.asp?id=15028).

54. AI-5 or Institutional Act Number 5, was a decree imposed by the military regimen in December 13 of 1968 that revoked most of the freedoms of Brazilian society and is still to this day remembered as the very face of the military dictatorship.

55. At this point there are two similar PL (Law Projects) with the same objective, the 84/1999 and the 587/2011.

56. The words used indistinctly by the media, **and in this law proposition**, actually have two different meanings, hacker being the really knowledgeable computer specialist and cracker

The clash of this OSS mentality with PSDB<sup>57</sup> proposition for regulating on-line activities and crimes, gave birth – as a counter measure from PT – to the idea of the Marco Civil<sup>58</sup>. This way one can understand not only from where does this law proposition came from, but also why it was designed in public like a free software project.

It is important to remember that Marco Civil is just a law proposition, it will later be submitted to the Congress where it might suffer alterations and it will be the topic of disputed negotiations amongst the parties. This legislative process might be the reason behind why the logs keeping proposition where maintained, even under heavy criticism. It looks like a political maneuver, trying to contemplate a portion of the other parties agenda.

### Control arguments and counter-arguments

Some of the arguments of logs supporters are that they are necessary to maintain the “*crime scene*” for a possible investigation that might rise in future. The problem with this argument is that there will be the preservation of a hypothetical “*crime scene*” without the knowledge that any *crime*<sup>59</sup> had ever took place.

Brazilian law does not allow previous recordings of logs, as already pointed, this recordings would constitute a breach of communications secrecy, a constitutional right, that can only be broke if ordered by a judge in course of a investigation. The 9.296/96 law in its Art. 2<sup>nd</sup> defines that if “there are no reasonable evidence of authorship or participation in penal infraction” and “the evidence could be generated by other means available” the interception of communications will not be admitted. The very maintenance of access logs at the ISP is against this same law, that limits even authorized monitoring of communications to exceed no more than 15 days, renewable by the same period. It is also possible to argue that the prohibition of log maintenance is in the best interest of very fundamental human rights. It is not correct to record communications, or keep of logs, on the very basic concept that one person is innocent until proven guilt.

---

the person who perpetrates illegal actions as invasions and software cracking.

57. PSDB is the major opposing party in Brazil, and also the ex-government party.

58. There is a considerable overlap of intentions and actors between the Marco Civil and New LDA initiatives.

59. There should be stated that there is a difference between a crime and a transgression, the crime bares within itself a much higher offensive degree. The italics is to point that Hardly a crime can take place over the Internet, most of the time the illegal actions via Internet are transgressions.

Presumption of innocence is a basic milestone of the majority of constituted legal systems and, together with privacy, is a fundamental right for a democracy. The simple knowledge that all communications and interactions that occur over the Internet are being logged, can have a profound chilling effect on democracy and free-speech. It would also be a law unable to fulfill its intended purposes, since tech savvy users can easily defeat such monitoring, or worst, can easily frame other people, forging or interfering in logs generation.

This kind of control proposition exists only due to the technical viability of their implementation, they are not difficult and neither extremely costly to implement, this way they present a great temptation for certain economic groups and reactionary politicians, whom would consider it a fair trade, to loose some democratic values in exchange of bigger control over Internet communications. Their discourses defending the reasons to sacrifice citizens freedoms are, invariably, disguised as very fundamental security concerns, that would be in the best interest of the citizens to support.

A good example are in the law projects PL-84/1999<sup>60</sup> and PL-587/2011<sup>61</sup> now in Congress that “Deals with the crimes committed in the area of informatics, its penalties and other measures”, “Characterizes as virtual or computer crime the attacks perpetrated by hackers and crackers, especially the manipulations of home pages and the misuse of passwords”, and “Deals with the classification of the criminal conduct on the Internet and other measures.”

A fundamental aspect to be observed here is that today, the Brazilian state can legally keep logs and can legally investigate citizens if security concerns rise, but only after the beginning of an investigation and when ordered by a judge. Such process is intended to preserve the two fundamental constitutional principles of privacy and presumption of innocence. These law projects mentioned, try to eliminate this need by creating a course of actions much more direct, conducted by the police.

It is also important to mention that today, the ISP already do keep access logs for alleged *security reasons*, any ISP making use of Proxy servers do know exactly who the user is, what it has accessed in a determined moment and what files were delivered to the user during connection, and today, there are logs generation and keeping by the ISP for “control reasons”, not always under ideal security conditions, a recurring argument used by those who try to avoid logs keeping.

---

60. “Lei Azeredo”.

61. “PL-587/2011”, [s.d.], [http://www.camara.gov.br/sileg/Prop\\_Detalhe.asp?id=493377](http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=493377).

## Some weird court decisions

Another area where Brazilian civil rights seems to be under pressure is in the matters of free-speech. Even considering it would drive this text away from the current law propositions, it seems an important subject to be mentioned, since the Internet is the dwelling space where free-speech is being challenged. Just to illustrate the situation we will take a look at some weird court decisions involving free-speech.

We have already pointed out that Art. 5<sup>th</sup> of the Constitution, on Item IV states that: *“The manifestation of thinking is free, but anonymity is forbidden”*, and this same article, in Item V assures right to answer, and even material reparation in cases of material, moral or image damages. We can extrapolate one explanation by inferring that the legislators reasoning would be freedom with responsibility.

The same article, in Item IX grants right to free expression, and intellectual, artistic, scientific and communication freedoms, that should not face any kind of censorship or licensing interferences, Item X made it inviolable the intimacy, private life, honor and image of the person, again, reassuring possibility of compensation for material or moral damages if violations occur.

This way *“honor and image”* are solid constitutional guarantees, that would not be affected by freedom of expression since anonymity is forbidden, and compensation for material or moral damages are also assured in cases of any violation.

Also, as already explained, the Brazilian law is hierarchically organized, and the *“Constitution rule above all the other laws, and no law can go against it, or it will be labeled unconstitutional and, theoretically, put to no effect”*.

Principles established, it is possible to test them against real cases. Lets us check two cases involving the two biggest newspapers of Brazil: O Estado de São Paulo (Estado) and Folha de São Paulo (Folha).

The first one is related to Folha, and is really a direct test for Item IX that *“grants the right to free expression”* assuring that one *“should not face any kind of censorship or licensing interferences”*. In Portuguese the word *Folha* is a synonym for daily newspaper, but it is just one letter from *fAlha* that means *fail* in Portuguese. A site named *“Falha de São Paulo”*, with an *a*, has been taken off the Internet, by newspaper *Folha* under allegations of *“misuse of the trademark”* in a polemical decision, seen by many as an act of censorship. Even putting aside the free-speech issue, the defendants presented themselves as being a parody site, and parody is

protected by the Brazilian copyright law<sup>62</sup>, it made no difference as they were ordered to stop their activities.

The second case got an additional twist, that brings some understanding of how free-speech is not a strong value in contemporary Brazil. The *Estadão* is, for over one year now, prohibited by a judge of publishing an array of informations, including content of phone calls, from members of the ex-President Sarney<sup>63</sup> and about himself. Even without any consideration about the content of this materials, this act is seen as a “*prior censorship*”<sup>64</sup> and is unconstitutional; the correct procedure for the justice would be to let the paper publish the informations it got and then, if someone is offended, they can ask the justice to evaluate if it constituted any offense at all, in a positive case it could generate compensation and the right of answer. On the front cover of the *Estadão* website the paper keeps a black stripe and a counter updated every day, showing to all visitors, for how long it has been under censorship<sup>65</sup>.

That is the reason why so many people got extremely surprised when the analyst Maria Rita Kell, writer of this same newspaper, got fired (in 02/10/2011) by the *Estadão*<sup>66</sup>, after publishing an opinion column in the paper, criticizing the élites and supporting President Lula.

Examples like these abound in contemporary Brazilian society, and they extend to both sides of the political spectrum, including censorship initiatives originated within PT members<sup>67</sup>.

---

62. Art. 47. São livres as paráfrases e paródias que não forem verdadeiras reproduções da obra originária nem lhe implicarem descrédito. / Article 47.Paraphrases and parodies are free when they are not true reproductions of the original work nor does imply disbelief to it.

63. “Justiça censura Estado e proíbe informações sobre Sarney - política - Estadão.com.br”, [s.d.], <http://www.estadao.com.br/noticias/nacional,justica-censura-estado-e-proibe-informacoes-sobre-sarney,411711,0.htm>.

64. “Entidades da área de imprensa denunciam ‘censura prévia’ - política - Estadão.com.br”, [s.d.], <http://www.estadao.com.br/noticias/nacional,entidades-da-area-de-imprensa-denunciam-censura-previa,411761,0.htm>.

65. “1 ano sob censura - Especiais :: Estadão.com.br”, [s.d.], <http://www.estadao.com.br/pages/especiais/sobcensura/>.

66. “Maria Rita Kehl: ‘Fui demitida por um “delito” de opinião’ - Terra - Política”, [s.d.], <http://terramagazine.terra.com.br/interna/0,,OI4722228-EI6578,00-Maria+Rita+Kehl+Fui+demitida+por+um+delito+de+opinio.html>.

67. “Entrevista de Marta: Cabral repudia censura à imprensa - O Globo Online”, [s.d.], [http://oglobo.globo.com/pais/mat/2008/06/18/entrevista\\_de\\_marta\\_cabral\\_repudia\\_censura\\_imprensa-546864302.asp](http://oglobo.globo.com/pais/mat/2008/06/18/entrevista_de_marta_cabral_repudia_censura_imprensa-546864302.asp); “Juiz eleitoral autoriza censura prévia em SC - Terra - Política”, [s.d.], <http://terramagazine.terra.com.br/interna/0,,OI3219344-EI6578,00.html>; “STF

## Conclusions

The original idea of this text was to evaluate if Brazil can conduce a democratic creation of laws regarding the new communication technologies without hurting consolidated civil rights. Three major issues emerge as constitutional rights not fully preserved, defended or that are somehow endangered: the free manifestation of thinking, the privacy and freedom of communications, the access to cultural goods.

The free manifestation of thinking is now under attack by two significant threats, the disposition of tribunals to enter in the realm of opinion litigations, usually against bloggers at left and right, and the very unsettling *prior censorship*, usually granted to politicians.

Privacy and freedom of communications are under attack by different law propositions and even by the Marco Civil, once the official sanction to logs keeping initiatives will grant the state the power to scrutinize citizens activities, under many different precedents; also it will grant the state the incredible power to go back in time, to investigate alleged *crimes* committed in the past and kept crystallized in computer logs. This initiatives can have a profound chilling effect in many levels of free-speech and even in the very ability of the citizen to criticize and oversee government actions.

Copyright law in Brazil already is one of the most restrictive in the world, it functions as a legal wall, used to keep citizens detached of education and cultural development, the economic status being the central factor to define how, and in what extent, the citizen can access cultural goods. The current reform proposition of the 9.610/98 law was made to amend this situation and have good chances of achieving its goals. It remains to be seen if it will survive the legislative process inside the Congress.

Finally we can say that long time conservative interest groups and leftist-oriented intelligentsia are just the surface, and the most obvious aspect of the normative and social challenges that new communication technologies are presenting to Brazilian society.

This challenges run across right winged parties like PSDB and PFL, the supporters of copyright industries, religious groups, NGOs, left winged parties like PT, and

---

considera 'censura prévia' falta de acesso a dados de Dilma | Reinaldo Azevedo - Blog - VEJA.com", [s.d.], <http://veja.abril.com.br/blog/reinaldo/geral/stf-considera-censura-previa-falta-de-acesso-a-dados-de-dilma/>.

leftist-oriented activists from digital culture movements, OSS enthusiasts and many other interest groups.

At this point, even considering the innovations on how public debates are being conducted, the young Brazilian democracy looks really challenged in fulfilling the hopes for democratic creation of new laws, also it is no small task to harmonize the new legislation with civil rights already in place. These new laws will be instituted and that they will, somehow, regulate the technological development of the country in the near future, it remains a question to be seen if current civil rights will survive the debates.

A famous Brazilian humorist, Millôr Fernandes, has once said: “A disgrace never comes alone. In Brazil it is always accompanied by threats to democracy”<sup>68</sup>.

## References

“1 ano sob censura - Especiais :: Estadão.com.br”, [s.d.]. <http://www.estadao.com.br/pages/especiais/sobcensura/>.

“A esquerda no poder local: Porto Alegre e o Partido dos Trabalhadores”, setembro 12, 2009. <http://www.ub.es/geocrit/sn/sn-24516.htm>.

Basso, Maristela. “O Regime Internacional de Proteção da Propriedade Intelectual da OMC/TRIPS”. In *OMC e Comércio Internacional*, organizado por Alberto do Amaral Júnior, 360. São Paulo: Aduaneiras, 2006.

Bevilaqua, Clovis, e Aquiles Bevilaqua. *Código Civil Dos Estados Unidos Do Brasil Commentado*. Vol. 3. 9th ed. Rio de Janeiro: Francisco Alves, 1916.

Bono, Sonny. *Sonny Bono Copyright Term Extension Act*, 1998. [www.copyright.gov/legislation/s505.pdf](http://www.copyright.gov/legislation/s505.pdf).

“Constituição da República dos Estados Unidos do Brasil de 1891”, [s.d.]. [http://www.planalto.gov.br/ccivil\\_03/constituicao/Constitui%C3%A7%C3%A3o.htm](http://www.planalto.gov.br/ccivil_03/constituicao/Constitui%C3%A7%C3%A3o.htm).

*Constituição da República Federativa do Brasil de 1988*. *Constituição da República Federativa do Brasil de 1988*, 1988. [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao/constituicao/Constitui%C3%A7%C3%A3o.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao/constituicao/Constitui%C3%A7%C3%A3o.htm).

“Consulta Direito Autoral”, [s.d.]. <http://www.cultura.gov.br/consultadireitoautoral/consulta/>.

Consumers International. *Consumers International IP Watchlist 2011*. Consumers International, 2011. <http://A2Knetwork.org>.

---

68. «Uma desgraça nunca vem só. No Brasil vem sempre acompanhada de ameaças à democracia.» in <http://twitter.com/millorfernandes/status/6760821167>.

“Debate Público Proteção de Dados Pessoais”, [s.d.]. <http://culturadigital.br/dadospessoais/apresentacao-2/>.

“Dilma Rousseff — Presidência da República Federativa do Brasil”, [s.d.]. [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/dilma-rousseff](http://www.presidencia.gov.br/info_historicas/galeria_pres/dilma-rousseff).

“Entidades da área de imprensa denunciam ‘censura prévia’ - política - Estadão.com.br”, [s.d.]. <http://www.estadao.com.br/noticias/nacional,entidades-da-area-de-imprensa-denunciam-censura-previa,411761,0.htm>.

“Entrevista de Marta: Cabral repudia censura à imprensa - O Globo Online”, [s.d.]. [http://oglobo.globo.com/pais/mat/2008/06/18/entrevista\\_de\\_marta\\_cabral\\_repudia\\_censura\\_imprensa-546864302.asp](http://oglobo.globo.com/pais/mat/2008/06/18/entrevista_de_marta_cabral_repudia_censura_imprensa-546864302.asp).

Erber, Georg. “Proprietary Digital Rights Management Systems and Music-Downloads - Obstacles for Innovation from a Competition Policy Perspective”. *SSRN eLibrary* (setembro 18, 2009). [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1475059](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1475059).

“Fernando Afonso Collor de Mello — Presidência da República Federativa do Brasil”, [s.d.]. [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/gal-collor](http://www.presidencia.gov.br/info_historicas/galeria_pres/gal-collor).

“Fernando Henrique Cardoso (2) — Presidência da República Federativa do Brasil”, [s.d.]. [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/galfhc](http://www.presidencia.gov.br/info_historicas/galeria_pres/galfhc).

“Fernando Henrique Cardoso — Presidência da República Federativa do Brasil”, [s.d.]. [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/galfhc1](http://www.presidencia.gov.br/info_historicas/galeria_pres/galfhc1).

“Gilberto Gil: ‘Pirataria é desobediência civil’ - Terra - Cultura”, março 5, 2009. <http://terramagazine.terra.com.br/interna/0,,OI3605448-EI6581,00-Gilberto+Gil+Pirataria+e+desobediencia+civil.html>.

“Itamar Augusto Cautiero Franco — Presidência da República Federativa do Brasil”, [s.d.]. [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/galita-mar](http://www.presidencia.gov.br/info_historicas/galeria_pres/galita-mar).

Jancsó, István, org. *Cronologia de História do Brasil Colonial (1500-1831)*. Série Iniciação 1. São Paulo: FFLCH-USP, 1994.

“José Ribamar Ferreira de Araújo Costa - José Sarney — Presidência da República Federativa do Brasil”, [s.d.]. [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/galsarney](http://www.presidencia.gov.br/info_historicas/galeria_pres/galsarney).

“Juiz eleitoral autoriza censura prévia em SC - Terra - Política”, [s.d.]. <http://terramagazine.terra.com.br/interna/0,,OI3219344-EI6578,00.html>.



“Justiça censura Estado e proíbe informações sobre Sarney - politica - Estadão.com.br”, [s.d.]. <http://www.estadao.com.br/noticias/nacional,justica-censura-estado-e-proibe-informacoes-sobre-sarney,411711,0.htm>.

“Luiz Inácio Lula da Silva (2) — Presidência da República Federativa do Brasil”, [s.d.]. [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/Lula2](http://www.presidencia.gov.br/info_historicas/galeria_pres/Lula2).

“Luiz Inácio Lula da Silva — Presidência da República Federativa do Brasil”, [s.d.]. [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/Lula](http://www.presidencia.gov.br/info_historicas/galeria_pres/Lula).

“Marco Civil”, [s.d.]. <http://culturadigital.br/marcocivil/sobre/>.

“Maria Rita Kehl: ‘Fui demitida por um “delito” de opinião’ - Terra - Política”, [s.d.]. <http://terramagazine.terra.com.br/interna/0,,OI4722228-EI6578,00-Maria+Rita+Kehl+Fui+demitida+por+um+delito+de+opiniao.html>.

Marques, Ivan da Costa. “Cloning Computers: From Rights of Possession to Rights of Creation”. *Science as Culture* 14 (2) (junho 2005): 139-160.

Martinez, Paulo Henrique. “O Partido dos Trabalhadores e a Conquista do Estado 1980-2005”. In *História do Marxismo no Brasil - Partidos e movimentos após os anos 1960*, 6:464. Campinas: Editora da UNICAMP, 2007.

Oliveira, Orlandina de, e Bryan Roberts. “O Crescimento Urbano e a Estrutura Social Urbana na América Latina, 1930-1990”. In *História da América Latina: a América Latina após 1930: Economia e Sociedade*, VI:560. São Paulo: Edusp, 2005.

Paranaguá, Pedro, e Sérgio Branco. *Direitos Autorais*. 1st ed. FGV Jurídica. Rio de Janeiro: Editora FGV, 2009.

“PL-587/2011”, [s.d.]. [http://www.camara.gov.br/sileg/Prop\\_Detalhe.asp?id=493377](http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=493377).

“PL-84/1999”, fevereiro 24, 1999. [http://www.camara.gov.br/sileg/prop\\_detalhe.asp?id=15028](http://www.camara.gov.br/sileg/prop_detalhe.asp?id=15028).

“Quem tem medo da mudança?” *Link - Estadão.com.br*, março 20, 2011. <http://blogs.estadao.com.br/link/quem-tem-medo-da-mudanca/>.

Reis, Daniel Aarão. “Entre Reforma e Revolução a Trajetória do Partido Comunista no Brasil entre 1943 e 1964”. In *História do Marxismo no Brasil - Partidos e organizações dos anos 1920 aos 1960*, 5:304. Campinas: Editora da UNICAMP, 2007.

Silva, Sergio. *Expansão Cafeteira e Origens da Indústria no Brasil*. São Paulo: Alfa-Omega, 1976.

“STF considera ‘censura prévia’ falta de acesso a dados de Dilma | Reinaldo Azevedo - Blog - VEJA.com”, [s.d.]. <http://veja.abril.com.br/blog/reinaldo/geral/stf-considera-censura-previa-falta-de-acesso-a-dados-de-dilma/>.

“Tancredo de Almeida Neves — Presidência da República Federativa do Brasil”, [s.d.]. [http://www.presidencia.gov.br/info\\_historicas/galeria\\_pres/galtancredo](http://www.presidencia.gov.br/info_historicas/galeria_pres/galtancredo).

Todd Benson. “Brazil - Free Software’s Biggest and Best Friend”. Imprensa. *NY-Times.com*, março 29, 2005. [http://select.nytimes.com/gst/abstract.html?res=F40614FD395B0C7A8EDDAA0894DD404482&fta=y&incamp=archive:article\\_related](http://select.nytimes.com/gst/abstract.html?res=F40614FD395B0C7A8EDDAA0894DD404482&fta=y&incamp=archive:article_related).

# **Passage of freedom of information bill in Nigeria: the unending journey**

---

**Mercy Ifeyinwa Anyaegbu &  
Rose Obiozor-Ekeze**

---

## **Introduction**

Information has become the essential tool in the development process, in enhancing good governance and empowering people around the world. Unfortunately, virtually all government information in Nigeria is classified as top secret. This veil of secrecy makes it difficult to get information from any state agency. A plethora of laws prevent civil servants and other government officials from divulging official facts and figures. These laws include the Official Secrets Act, Criminal Code, Evidence Act, Public Complaint Commission Act, Statistics Act, Civil Service Rules etc. These officials including journalists are required upon appointment to swear an oath of secrecy not to disclose any information that comes their way unless specifically authorized to do so.

The idea behind these laws is to protect vital government information but the level of secrecy is so ridiculous that some classified government files contain ordinary information like newspaper cuttings which are already in the public domain. Freedom of Information Bill is a bill which if passed into law will give every Nigerian a legal right of access to information, records, and documents held by the government or its agency. In Nigeria this bill was first submitted to the National Assembly in 1999. The continued delay in the passage of this bill by the National Assembly has continued to attract mixed reactions from stakeholders. This paper x-rayed its legislative history; examined the impediments, provisions, adequacy, weaknesses, public outcry and input of different interest groups. Recommendation was based on issues thereof.

## **Idea of Classified Information**

Classified information is information which has been deemed sensitive enough that access to it is restricted. A classic example of classified information is military intelligence circulated only among the people who absolutely need to see to it to reduce the risk of potentially catastrophic leaks of information. All governments and many large corporations have systems in place for identifying and se-

curing classified information to ensure that it does not fall into the wrong hands (Switch, 2010).

In Nigeria, Rule 010103 of the Public Service Rules of 2006, define classified correspondence to mean “correspondence which has been graded Restricted, Confidential, Secret or Top Secret” Most governments differentiate their classified information into several levels, ranging from top secret information which is only seen by a handful of people to unclassified information which is open to the general public. When information is evaluated to determine whether or not it should be classified, the primary concern is national security. Willful disclosure of information to the enemy is generally considered as treason. People who work for the government receive a security clearance which details the information they can access.

Rule 030415 of the Public Service Rule makes it mandatory for every permanent secretary/head of extra-ministerial office to ensure that all officers, employees and temporary staff under his control who have access to classified or restricted papers to sign the Oath of Secrecy in the appropriate form before they are granted such access and such declarations are safely preserved.

## **Laws Inhibiting Free Access to Information in Nigeria:**

### ***1. Official Secrets Act***

Classified matter under this Act means ‘any information or thing which, under any system of security classification, from time to time, in use by or by any branch of the government, is not to be disclosed to the public and of which the disclosure to the public would be prejudicial to the security of Nigeria’.

A cursory look at the provisions of this Act would reveal that any person who

- a) transmits any classified matter to a person to whom he is not authorized on behalf of the government to transmit it or
- b) obtains, reproduces or retains any classified matter which he is not authorized on behalf of the government to obtain, reproduce or retain, as the case may be, is guilty of an offence.

Furthermore, in Section 1 (2) ‘A public officer who fails to comply with any institutions given to him on behalf of the government as to the safeguarding of any classified matter which by virtue of his office is obtained by him or under his control is guilty of an offence’.

### **Protection of Defence Establishments**

In Section 2 (1) A person who for any purpose prejudicial to the security of Nigeria-

- a) enters or is in the vicinity of or inspects a protected place; or
- b) photographs, sketches or in any other manner whatsoever makes a record of the description of, or of anything situated in, a protected place; or
- c) obstructs, misleads or otherwise interferes with a person engaged in guarding a protected place; or
- d) obtains, reproduces or retains any photograph, sketch, plan, model or document relating to, or to anything situated in, a protected place, is guilty of an offence.

#### Restrictions on Photograph, etc During Periods Of Emergency

##### Under Section 3 (1)

No person shall, without permission in writing given by the president, photograph, sketch, or in any other manner whatsoever make a record of the description of such things designed or adapted for use for defence purposes as may be specified by the order.<sup>6</sup>

In Section 2 (2) a person who contravenes the provisions of an order under this section is guilty of an offence.

## **2. The Criminal Code Act**

Section 97 deals with-Disclosure of official secrets and states:

- 1) Any person who, being employed in the public service, publishes or communicate any fact which comes to his knowledge by virtue of his office, and which it is his duty to keep secret, or any document which comes to his possession by virtue of his office and which it is his duty to keep secret, except to some person to whom he is bound or communicate it, is guilty of a misdemeanor, and is liable to imprisonment for two years.
- 2) Any person who, being employed in the public service, without proper authority abstracts, or makes a copy of, any document the property of his employer is guilty of a misdemeanor and is liable to imprisonment for one year.

## **3. The Evidence Act**

Section 109 defines the following as public documents:

- a) documents forming the acts or records of the acts:
  - i) of the sovereign authority;
  - ii) of official bodies and tribunals; and
  - iii) of public officers, legislative, judicial and executive, whether of Nigeria or elsewhere;
- b) public records kept in Nigeria of private documents.

Section 168 states that:

‘No public officer shall be compelled to disclose communications made to him in official confidence, when he considers that the public interests would suffer by the disclosure’.

This is further amplified in Section 175:

No one shall be compelled to produce documents in his possession which any other person would be entitled to refuse to produce if they were in his possession, unless such last mentioned consents to their production.

#### ***4. The Public Complaints Commission Act***

This Act was established in 1975 with wide powers to inquire into complaints by members of the public concerning the administrative action of any public authority and companies or their officials, and other matters ancillary thereto.

Under section 5 of this Act, a commissioner shall have power to investigate either on his own initiative or following complaints lodged before him by any other person, any administrative action taken by-

- a) any Department or Ministry of the Federal or any State Government;
- b) any Department of any local government authority set up in any State in the federation;
- c) any statutory corporation or public institution set up by any Government in Nigeria;
- d) any company incorporated under or pursuant to the companies and Allied Matters Act whether owned by any Government aforesaid or by Private individuals in Nigeria or otherwise however; or
- e) any officer or servant of any of the aforementioned bodies.

Pursuant to these, the Act empowers any Commissioner in Section 3 (c) to have access to all information necessary for the efficient performance of his duties under this Act and for this purpose may visit and inspect any premises belonging to any person or body mentioned in subsection 2 above.

Although this Act made adequate provision for its officers to have unrestricted access to any information that may be inquired in the course of their duty, such unrestricted access is disallowed in the disclosure of the commission’s result of investigation. It is stated categorically in Section 5 (5) that

- All Commissioners and all the staff of the commission shall maintain secrecy in respect of matters so designated by reason of source or content, so however that a commissioner may, in any report made by him, disclose such matters as in his

opinion ought to be disclosed in order to establish grounds for his conclusions and recommendations.

In Section 6, a commissioner is prevented from investigating any matter that is pending before a court of law or the National Assembly or any act purported to have been done in respect of any member of the armed forces in Nigeria or the Nigeria Police Force.

Furthermore, in Section 8 (1) any compliant lodged before the Commissioner shall not be made public by any person except a commissioner. Any person who contravenes the provisions of this subsection shall be guilty of an offence and shall be liable upon conviction to a fine of N5000 or imprisonment for a term of six months or both such fine and imprisonment.

The officers of this Commissioner enjoy immunity from legal process as stated in section 10 (2)-

Any report, statement or other communication or record of any meeting, investigation or proceedings which a Commissioner, officer or servant of the Commission may make in the exercise of his functions under this Act, shall be privileged in that its production may not be compelled in any legal proceedings if the Attorney – General of the Federation certifies that such production is not in the public interest.

### **5. The Public Service Rule**

Under Rule 030416 of the PSR, every officer is subject to the Official Secrets Act and is prohibited from disclosing to any person, except in accordance with official routine or with special permission of government, any article, note, document or information entrusted to him/her in confidence by any person holding office under any Government in the Federal Republic of Nigeria, or which he/she has obtained in the course of his/her official duties. Similarly, every officer shall exercise due care and diligence to prevent the knowledge of any such article, note, document or information being communicated to any person against the interest of the Government.

Furthermore, Rule 030402 (1) defines unauthorized disclosure of official information as a serious act of misconduct and the ultimate penalty for serious misconduct according to Rule 030407 is dismissal. The implication of dismissal for the officer is that he forfeits all claims to retiring benefits (Abioye, 2010).

#### **Copying And Removal of Records**

Rule 03417 of the PSR forbids a public officer from abstracting or copying official minutes, records or other documents except in accordance with official rou-

tine or with special permission of his Permanent Secretary / Head of Extra- Ministerial office.

- Access to Personal Records

According to Rule 030418, the general rule in Nigeria is that no public officer should have access to official and secret records relating personally to him.

- Publication and Public Utterances

Rule 030421 forbids a public officer except in pursuance of his/her official duty (even while on leave or leave of absence) to

- a) contribute to, whether anonymously or otherwise, publish in any newspaper, magazine or periodical or otherwise publish, cause to be published in any manner anything which may reasonably be regarded as of a political or administrative nature;
- b) speak in public or broadcast on any matter which may reasonably be regarded as of a political or administrative nature;
- c) allow himself / herself to be interviewed or express any opinion for publication on any question of a political or administrative nature or on matters affecting the administration, public policy, defence or military resources of the Federation or any other country.

In essence, these provisions were made to ensure that public officers are to be seen and not heard except when authorized in order to prevent vital information of government from being divulged through careless and unguarded utterances. They also confirm the age-long administrative practice under which the civil service is regarded as neutral and anonymous (Abioye, 2010).

## Concept of A Bill

The three arms of government in Nigeria consist of the executive, legislature and the judiciary. The legislature is represented by the National Assembly (Senate and House of Representatives) at the Federal level and state House of Assembly at the state level. The legislature performs three key functions – law making, representation and oversight. Primarily it assumes its importance as a law – making body. As enriched in Section 4 (2) of the 1999 constitution of the Federal Republic of Nigeria,

National Assembly shall have power to make laws for the peace, order and good government of the Federation or any part thereof with respect to any matter included in the Exclusive Legislative list set out in Part I of the second schedule to this constitution.



At the state level, the State House of Assembly is empowered in Section 7 of the Constitution to make laws for the peace, order and good government of the state or any part thereof. The power of the National Assembly to make laws shall be exercised by bills passed by both the Senate and House of Representatives and, except as otherwise provided by subsection (5) of this section, assented to by the President.

A bill in the context of legislation has been described as an idea for a new law, or an idea to change or do away with an existing law (Hamalai, 2010). In the Nigerian context, a bill is the draft of a proposed law to be discussed by the National Assembly or by a Senate House of Assembly. As noted before, the power to make bills derives from sections 58, 59 and 100 of the Nigerian Constitution. Such power is also subject to the legislative procedures under the Standing Rules / Orders of the Houses.

Proposal for a bill may emanate from a private citizen, business outfit, professional association / non-governmental group, special interest group or even a government unit. However, all bills must be sponsored by one or more legislators for it to be considered by the legislators. In Nigeria, bills enter the legislative process through the House of Representatives and Senate at the federal level and House of Assembly at the State level. At the Federal level, bills must pass through both chambers of National Assembly.

The bills drafted, considered and eventually passed into law cover various spheres of the economic, social, political and cultural lives of the Nigerian people.

## Types of Bills

As there are different sources of a bill so are there different types of bills. They include:

- Executive bill
- Members of the legislature bill (member's bill)
- Interest groups / Associations bill (also called private bills)
- Judiciary bills Another way of categorizing bill is by focus which consists of:
  - Public bills
  - Private bills
  - Hybrid bills

Finally bills may be classified according to financial implication. Thus there are

- Money bills (referring to definite matters in the constitution) S.80-84) and
- Ordinary bills (relates to matters not specified in the constitution).

## **Procedure for Passing a Bill in the National Assembly**

A Bill does not become law overnight. It undergoes through several stages until it has received the approval of the legislature and finally assented to by the President. These stages will be discussed hereunder

### **1. Receipt of Bill**

a) Bill from the Executive and Judiciary. According to Hamalai (2010), draft bills from the Executive and Judiciary are forwarded with a covering letter to both the President of the Senate and Speaker of the House of Representatives. Upon receipt, a copy of the bill is sent by the Presiding officer of each House to the Rules and Business committees.

b) Draft bills from Members of National Assembly. The member sponsoring the bill will forward it to the Senate President or the Speaker as the case may be. The Senate President or the Speaker will in turn send the bill to the Rules and Business committees for scheduling for First Reading and subsequent Readings.

### **2. Notice Regarding Bills**

Bills from the Executive, Judiciary and as well as members' bill are expected to be published in the official Gazette.

### **3. Readings/Stages of a Bill**

Every bill must receive three Readings before it is passed. Each Reading entails series of actions to be taken. For example, after the second Reading, the Bill must pass through a number of sub-stages before the Third Reading which is the Final Reading.

The various stages require appropriate time for scrutiny of the required activities.

### **Clean Bill**

When a Bill originating in either the Senate or House of Representative has been read the third time, a copy of it (incorporating all amendments) called a "clean copy", signed by the Clerk and endorsed by the Presiding officer is forwarded by the clerk of the originating house to the clerk of the other House with a message desiring the concurrence of the House receiving the bill.

- Where the amendments proposed by one House are acceptable to the other House (when the Bill has passed through all the required stages in the other House), the clerk of the House to which the Bill had been sent retains the Bill

and sends a message to the originating House indicating agreement to the bill without amendment.

- Where the Bill passed by one House is not agreed to by the other House or is agreed to with amendments to which the other House now seeks concurrence of the originating House, but the originating House does not concur to the other House's amendments, a conference of both Houses is then requested by the originating House. That is, where both Houses disagree on some issues, a conference committee is convened.

### **Conference Committee**

A conference committee is set up where the second chamber refuses to remove the changes it made. The conference committee which is made up of representatives of both chambers attempts to reconcile the differences and presents its recommendations in the form of a conference report. If this committee reaches a compromise and both chambers adopt the conference committee report, the Bill is once again voted on for passage. Essentially:

- Where both Houses agree in Conference and the conference reports are accepted by both Houses and all issues resolved, each House re-passes the Bill incorporating all conference amendments and endorsed by the Houses. Subsequently, all the original papers are transmitted to the clerk of the House in which the Bill originated for enrolment action.
- Where the two Houses fail to agree after a conference, then another conference committee may be appointed or the initiative dies in committee when the legislature adjourns.

Finally, when a bill has been passed in identical form by both Houses, a copy is prepared for the President's/Governor's assent as the case may be. The chief-Executive signs the Bill if he/she is satisfied (PARP, 2010)

### **Why Freedom of Information Law?**

Freedom of information legislation is rules that guarantee access to data held by the State. They establish a "right to know" legal process by which requests may be made for government-held information, to be received freely or at a minimal cost, barring standard exceptions.

Many countries exclude information in the domain of the private sector from their Freedom of Information bill. While some countries enact open meeting legislation which allows access to government meetings not just the records of them. In many countries, privacy or data protection laws may be part of the Freedom of

Information legislation. Most often Freedom of information laws does not allow disclosure of Information that affects national security, defence and other matters that are deemed of national interest.

Over 85 countries around the world have implemented some form of freedom of information legislation. Sweden has the oldest which was enacted in 1766.

Some African countries who have Freedom of Information law include South Africa, Mozambique, Liberia.

### **Salient Features of FOI Bill In Nigeria**

This Act seeks to provide a right of access to public information or records kept by government, public institution or private bodies carrying out public functions for citizens and on-citizens of the country.

This Act also seeks to increase the availability of public records and information to citizens of the country in order to participate more effectively in the making and administration of laws and policies and to promote accountability of public officers.

This bill provides in section 2 (1) that 'every citizen of the Federal Republic of Nigeria has a legally enforceable right to, and shall, on application, be given access to any record under the control of a government or public institutions'.

It further states in 2 (2) that the applicant does not need to demonstrate any specific interest in the information being applied for.

Section 3 (1) made it mandatory that the head of every government or public institution to which this Act applies shall cause to be published in the Federal gazette a description of:

- a) the organization and responsibilities of the institution including details of programmes and functions of each divisions, branch and department of the institution;
- b) all classes of record under the control of the institution in sufficient details to facilitate the exercise of the right to access under this Act;
- c) all manuals used by employees of the institution in administering or carrying out any of the programmes or activities of the institutions;
- d) Documents containing final opinions including concurring and dissenting opinions as well as orders made in the adjudication of cases;
- e) Documents containing substantive rules of the institution;

- f) Documents containing statements and interpretations of policy which have been adopted by the institution;
- g) Documents containing final planning policies, recommendations and decisions;
- h) Documents containing factual reports, inspection reports, and studies whether prepared by or for the institution;
- i) Documents containing information relating to the receipt or expenditure of public or other funds of the institution;
- j) Documents containing the names, salaries, titles and dates of employment of all employees and officers of the institution;
- k) Documents containing the rights of the state, the public, sub division of the state or a local government, or of any private person;
- l) Documents containing the name of every official and the final records of voting in all proceedings of the institutions;
- m) Files containing applications for any contract, permit, grant or agreement;
- n) A list of reports, documents, studies or publications prepared by independent contractors for the institution;
- o) Materials containing information relating to any grant or contract made by or between the institution or another government or public institution or private organization; and
- p) The title and address of the appropriate officers or employees of the institution to whom requests for access to records under this Act should be sent, provided that the failure of any government or public institution to publish any information required to be published under this subsection shall not prejudicially affect the right of access to public records and information in the custody of such government or public institution as provided for under this Act.

To ensure the reliability and validity of the above information, the Act provides in Section 3 (2) that the institution shall publish an update record when changes occur. Government or public institutions to which this Act applies as provided in Section 3 (4) are all authorities whether executive, legislative, or judicial agencies of the federal Government together with all companies in which a Federal, State or Local Government authority has a controlling interest and all private companies performing public functions.

Application for access to a record under this Act shall be made in writing and such request shall provide sufficient detail to enable an experienced employee of

the institution reasonable effort to identify the record (S.3 (4)). Response to such request shall commence not later than fourteen (14) working days from the date the application was received as provided in Section 5 (1).

Where access is denied, the head of the institution shall state in the notice the reason upon which the refusal was based and that the applicant has a right to have the decision reviewed by a court of competent jurisdiction (S.8 (1)).

Section 8 (2) further states that the notice of denial should contain the name of each person responsible for the denial and in Section 8 (3) the head of such institution is required to indicate whether such record exists in the institution.

### **Payment of Fees**

Payment of fees when access is granted according to Section 9 (1) (a) shall be limited to reasonable standard charges, for document search, or duplication, when records applied for is for commercial use. Same applies when records are not sought for commercial use and the application is made by an educational or non-commercial, scientific, research, or a representative of the news media (S.9 (1) (b)).

Section 9 (2) did provide that document shall be furnished without any charge or at a charge reduced below the fees established under Section 10 (1) (b) if disclosure of the information is in the public interest. That is, it will contribute significantly to the public understanding of the operations or activities of the government and not primarily in the commercial interest of the applicant.

The import of all fees prescribed in Section 9 is such that if any fee is to paid, the rationale for such payment will be to offset only the direct cost of search, duplication, reproduction, review or transcription.

### **Destruction/Falsification of Records**

Under Section 10, it is a criminal offence punishable on conviction to a maximum of three (3) years imprisonment for any officer or head of government or public institution to which this Act applies who ties to either willfully destroy any records kept in his/her custody or attempts to doctor or otherwise alter same before they are released to any person, entity or community applying for it.

### **Classified Information under the Act**

Certain categories of information are exempted from the general right of access. These include such information as: Defence/security matters, the conduct of international affairs, Law enforcement investigation, Trade secrets, Financial, com-

mercial, technical and scientific information of economic value. These are information the disclosure of which could reasonably be expected to be materially injuriously to the financial interest of the Federal republic of Nigeria or any state or Local government thereof, or the ability of the federal, State or Local Governments to manage its economy, or could reasonably be expected to result in an undue benefit to any person. These restrictions are contained in Sections 13-15 of the bill.

### **Personal Information**

The proposed Act under Section 16 empowers the head of a government or public institution to refuse to disclose any record applied for that contains personal information such personal information include:

- i) files and personal information maintained with respect to clients, patients, residents, students, other individuals receiving social, medical, educational, vocational, financial, directly from Federal agencies or government or public institution;
- ii) personnel files and personal information maintained with respect to employees, appointees or elected officials of any government or public institution or applicant for such positions;
- iii) files and personal information maintained with respect to any applicant, registrar or license by any government or public institution cooperating with or engaged in professional or occupational registration, licensure or discipline.
- iv) Information required of any tax payer in connection with the assessment or collection of any tax unless disclosure is otherwise applied for by state statute; and
- v) Information revealing the identity of persons who file complaints with or provide information to administrative, investigative, law enforcement, or penal agencies.

However under Section 16 (2) the head of a government or public institution may disclose any record applied for that contains personal information if

- a) the individual to whom it relates consents to the disclosure; or
- b) the information is publicly available.

Section 16 (3) allows disclosure if it would be in public interest and if such public interest outweighs the protection of the privacy of the individual to whom such information relates.

### **Third Party Information**

Further restriction of public records are contained in Section 17 (1-4) such classified information include trade secrets and allied matters, contractual relationships, proposal and bids for contract, grants, agreement, information that may frustrate procurement or give an advantage to any person;

Others include information on product of environmental testing carried out on behalf of government or public institution.

However under Section 17 (4), access may be given if the disclosure will be for public good as it pertains to public health, public safety or protection of the environment.

### **Advice/Personal Opinion**

Section 18 (1) forbids the disclosure of information that contains preliminary drafts, notes, recommendation, memoranda and other records in which opinions are expressed or policies or actions are formulated. This also applies to legislative documents; except if that aspect will be expunged before the document is publicly cited.

### **Legal Practitioner/Client Privilege**

Under Section 19 access is denied to records that contain information on legal practitioner/ client privileges.

### **Course or Research Materials**

Section 20 is for records that contain course materials or research prepared by faculty members.

Under Section 23, the head of a government or public institution may refuse to disclose any record applied for that contains information pertaining to:

- a) test questions, scoring keys and other examination data used to administer an academic examination or determine the qualifications of an application for a license or employment;
- b) architects' and engineers plans for building not constructed with public funds, to the extent that disclosure would compromise security and
- c) library circulation and other records identifying library users with specific materials.



## **Judicial Review**

Judicial review of administrative actions is provided for under Section 22 (1) and Section 22 (2). S.22 (1)

Any person who has been refused access to a record applied for, or part thereof may apply to the court for a review of the matter within thirty days after the head of government or public institution has refused or is deemed to have refused the application, or within such further time as the court may either before or after the expiration of those days fix or allow.

S.22 (2) An application made under this section shall be heard and determined summarily.

During prosecution, the burden of establishing that the head of a government or public institution is authorized to refuse the disclosure of a record under this Act or a part thereof shall be on the government or public institution concerned.

The court may order disclosure of the denied access as contained in Section 27 (1-2)

- i) if the court determines that the head of the government or public institution was not authorized to withhold access or
- ii) where the head of the institution is so authorized, but the court nevertheless determines that the head of the institution did not have reasonable grounds on which he refused to disclose the record or part thereof;
- iii) where the Court makes a findings that the interest of the public in having the record being made available is greater and more vital than the interest being served if the application is refused.

## **Records Not Covered by the Act**

Records not covered by this Act are contained in Section 28.

These include:

- a) published material or material available for purchase by the public
- b) library or museum material made or acquired and preserved solely for public reference or exhibition purposes; or
- c) material placed in the National Library, the National Museum or the non public section of the National Archives of the Federal Republic of Nigeria on behalf of any person or organization other than a government or institution.

## **Protection of Public Officers against Existing Laws**

Section 29 of the Freedom of Information bill in Nigeria made provision aimed at shielding public officers from a plethora of previous laws forbidding access to public documents. It states inter alia:

1) Notwithstanding anything contained in the Criminal Code, Penal code, Official Secrets Act, or any other enactment, no civil or criminal proceedings shall lie against any government or public institution, or against any person acting on behalf of the government or public institution, and no proceedings shall lie against the Federal Government, State or Local Government or any institution thereof, for the disclosure in good faith of any record or any part of a record pursuant to this Act, for any consequences that flow from that disclosure, or for the failure to give any notice required under this Act, if care is taken to give the required notice. Nothing contained in the Criminal Code or the Official Secret Act shall prejudicially affect any public officer who, without authorization discloses to any person, any public record or information which he reasonably believes to show-

- a) a violation of any law, rule or regulation;
- b) mismanagement, gross waste of funds, fraud, and abuse of authority; or
- c) a substantial and specific danger to public health or safety notwithstanding that such information was not disclosed pursuant to the provision of this Act.

2) No civil or criminal proceedings shall lie against any person receiving the information or further disclosing it.

In Section 30 further clarification is made for document which though may be classified as security document but not listed as such in Sections 14, 15, 16, 17, 18, 19, 20 or 21. Section 30 (1-3) states that such classification does not preclude such documents from being disclosed upon application except where the head of the institution deem it so.

## **Submission of Reports**

In Section 31, provision is made for sending of reports on or before February 1 of each year by each government or public institution. The essence of this report is to monitor progress and ensure compliance. Such reports must include:

- the number of applications such institutions turned down.
- number of appeals made and the reason adduced for denial.
- description of court decisions that upheld the denials made by the institutions as well as concise description of the scope of any information withheld.

- number of applications awaiting action as at 31<sup>st</sup> October of proceeding year and the median number of days such applications had waited.
- the number of applications so far received and the number processed.
- Median number of days it had taken the government or public institution to process different types of application
- total amount of fees collected to process all such application.
- the number of full-time staff of the Government or public institution devoted to processing applications for records, or the total amount expended by the Government or Public institution for processing such applications.
- S.31 (2) Each government or public institution shall make its report available to members of the public, even through online and other electronic means.
- This report shall be made to the Attorney General of the federation who shall in turn notify the National Assembly not later than April of same year and also ensure that such reports are available by electronic means.
- the AG of the Federation shall develop reporting and performance guidelines in connection with this report and may also establish additional requirement for such reports as he may determine.
- such report shall include a description of the effort taken by the Ministry of Justice to encourage all government or public institutions to comply with this Act.

## **The Legislative History of FOI in Nigeria**

The idea of a FOI law for Nigeria was conceived in 1993 by three different organizations, working independently of each other. The organizations, Media Rights Agenda, Civil Liberation Organization and the Nigerian Union of Journalists subsequently agreed to work together on a campaign for the enactment of a Freedom of Information Act. The “Draft Access to Public Records and information Act” produced by Media Rights Agenda in 1994 became the basis for further discussion and debates (<http://11234next.com/cps/cms/sites/Next/News/Natioanl/5679987-146/9-bills-long-journey> accessed /3/19/2011).

The FOI bill was first submitted to the National Assembly in July 1999 as a non-member bill by the Media Rights Agenda, a non governmental organization (Ogala, 2011). The document which had 34 sections was denied passage at the House of Representative as well as the Senate. It was recommitted in 2003 and was eventually passed in 2007 towards the closing session of that Parliament. The then President, Olusegun Obasanjo refused to sign it into law, citing national security infringement.

The bill was reintroduced in the National Assembly in 2007. It was sponsored by Abike Dabiri-Erewa, a former journalist. The passage of this bill has lingered since 2007. In February this year, the House of Representative eventually passed this bill which was renamed the “Right of Information Bill”, 2011”. The Senate passed its own version in March. Each chamber of the National Assembly passed a different version of the bill hence the need for conference committee where areas of differences will be harmonized before the President’s assent.

### **Public Outcry Against the Delay**

Part of the reasons adduced as impediments to accountability and transparency was the fact that the nation lacks an enabling law that gives the media and the citizenry unrestricted access to information on the dealings of government (Iriekpen & Obi, 2011). So one of the components of bargains put forward by the civil society and other pro-democracy groups at the advent of democracy was for an act that empowers the media and the people to hold their leaders accountable through having access to what happen within government circles-what comes in and goes out.

Commendable effort has been made by various interest groups towards the passage of this bill. These pressure groups include the Nigerian Labour Congress, Nigeria Union of Journalists, Nigerian Guild of Editors, Freedom of Information Coalition, Media Rights Agenda and other civil society groups. They have mounted a sustained campaign to make Nigeria join the league of other civilized societies by passing the bill.

### **Why the Long Delay in the Passage of FOI bill in Nigeria?**

The long delay in the passage of FOI bill in Nigeria can be attributed to the following:

#### ***1. Fear of the Press***

There is a widely-held view especially at the government circle (including the National Assembly) that FOI is a media bill which if passed into law will give journalists unchecked powers to abuse and misuse information that comes into their hands. According to Hon. Abike Dabiri (2008), there is a misconception that it is a bill that will make the press so powerful. Thus the Nigerian government is wary of enacting a law that may turn out to be its nemesis and a handy weapon in the arsenal of its enemy.

## ***2. Incompetence Exposed***

Those in government are fearful that a FOI act will enable the governed to be able to ascertain incompetence, wastefulness and corruption in government. Similarly, those in society are uncertain because they are unsure of how the provisions of the FOI will be implemented in Nigeria polity where instances of disregard of individual basic rights under laws by institutions and law enforcement agents are rife and where costly litigation may be required to enforce such rights.

## ***3. Apathy among Legislators***

When a bill is introduced in the National Assembly, the expectation is that support would be mobilized for it. Sometimes an interest group is expected to shore up support for the Bill. When the reverse is the case, the Bill becomes an orphan and its journey to passage may become protracted. Until recently, the FOI bill has not enjoyed the blessing of many members of the National assembly.

## ***4. High rate turnover of Legislators***

The life history of a bill if not passed into law is halted after every legislative session. Even when the interest in the bill is sustained at the commencement of a new session, it has to go through the same process as before since not all the law makers in the present house participated in the previous debate. Such is the case with FOI bill in Nigeria.

## ***5. Assent to Bills***

When the National Assembly passes a bill, it is still not a law until the President signs it. Where this assent is withheld, the bill may be sent back to the National Assembly; who may decide to put it to vote. Where a two third majority votes in favour of the bill, it becomes a law, if not the bill either dies a natural death or awaits another torturous journey. That was what happened between 1999 – 2004.

## ***6. Concurrent requirement for Bills***

Before assent is given by the president, both chambers of the National Assembly must pass a harmonized version of the bill. Where there is disagreement, it helps to prolong the passage of the bill. Presently, the FOI bill passed in Nigeria by the Senate and House of Representative differ hence the need for a conference committee before the President' assent.

## **Weakness/Lapses in Right of Information Bill in Nigeria**

A cursory look at the provisions of this bill will reveal some obvious lapses. In Section 15, the bill excludes economic and defence matters from the areas to which the public might have full access. The government shall refuse access to “(a) trade secret, financial, commercial or technical information that belongs to the government that has substantial economic value or is likely to have substantial value; and (c) proposal and bids for any contract, grants or agreement, including information which if it were disclosed would frustrate procurement or give an advantage to any person.

- 1) Adhering strictly to this provision means that Nigerian would have no right to know exactly how the money budgeted annually is spent, who and who are getting the contracts, and the parameter used in allocating resources.
- 2) Since information concerning the military remains a classified one the army in shielded from public scrutiny. This can encourage corruption and impunity.
- 3) The eleven years legislative struggle in the passage of this bill has not ended. The passage of the bill is yet to be harmonized and assented to by the President even when the tenure of the present parliament will end in May. Until this bill is signed into law and made public, Nigerians cannot for sure know whether it has satisfied the yearnings of the masses.
- 4) The bill made provision for legal action when access is denied. The impracticability of this facility stares one in the face. Access to justice in Nigeria is not an easy one. Similarly with the frequent industrial action all over the country, getting quick relief from the court may not be all that easy.
- 5) Provisions made to ensure access to information in the bill are laudable but it has far reaching implication. It will entail increase in labour force, improving the facilities of the government and public institutions, setting up of monitoring team that will monitor progress and compliance.
- 6) No provision is made for periodic review of the provisions of the law.

## **Recommendation**

Based on lapses so far x-rayed, the following recommendations are made:

1. Nigeria should borrow a leaf from India which has successfully transferred most of its record into electronic format. There has to be a major ICT initiative throughout the country; while steady supply of electricity is an imperative.

2. Public awareness – Not every citizen of Nigeria is aware of the rights inherent in the Right to Information Bill. There is need for sensitization of the citizenry.
3. Manpower Development-By time we have the law, there should be trained government officials who will be responsible for handling FOI requests.
4. The overriding influences in the disclosure of any public information/record should be public interest even if such document is classified.
5. The denial of access to public document may result in legal action, and as such legal action may increase with time, a special court may be created to handle all such cases. This is to ensure speedy disposal action.
6. Effort should be made by all state holders to ensure that the passage of this bill do not exceed this legislative session which will end in May.
7. The government should be proactive in the implementation of the provisions of this law. This it can do by setting up a monitoring committee. The monitoring committee should be a creation of the law.
8. To check abuse, the offence of libel may be made a criminal offence so that people become conscious of how they mismanage information.
9. Provision should be made for periodic review of every provision of the law.
10. Once the bill finally becomes a law, a plan of action should be put in place to review, amend or repeal all existing laws which impede access to information. New laws should be made to align with the provisions of Right to Information Law.

## Conclusion

Corruption thrives in secrecy. Passage of Freedom of Information bill in Nigeria which started in 1999 is one single bill with the longest legislative history. As at 31<sup>st</sup> March, 2011, this bill is still before the National Assembly. It is if it is passed into law, it will give every Nigerian a legal right of access to information, records and documents held by the government or its agency. There are some exemptions in the provisions of the new law. But these exemptions are in recognition of the fact that no government no matter how liberal will allow access to all kinds of information in its custody without some interest being jeopardized. Be that as it may, the continued delay in the passage of the bill has continued to attract mixed reaction from the entire Nigerian public. Both the media and other civil society groups have mounted a sustained campaign to ensure that this bill is passed into law.

## References

Abioye, Abiola (2010) 'Confidentiality and protection of official records in the freedom of information era: Nigeria' situation' *African Journal of Library, Archives and Information Science*. April 2010, 2.

Criminal Code Cap 11 Laws of the Federation of Nigeria, 2004

Erewa-dabiri, Abike (2008) House Representatives throws out FOI bill <<http://www.foicoalition.org/news/2008/repsthrwout.htm>> Accessed 09.01.2011

Evidence Act, Cap E14, Laws of the Federation of Nigeria, 2004

Freedom of information legislation <<http://en.wikipedia.org/wiki/freedom-of-information-legislation>>. Accessed 1/10/2011.

Hamalai, Ladi (2010) 10 years of law making in Nigeria, Abuja: PARP, 4.

Iriekpen, David and Obi, Paul 'FOI bill shifts to senate' *ThisDay* 1 March, 2011, 20.

Official Secrets Act, Cap 03, Laws of the Federation of Nigeria, 2004.

Ogala, Emmanuel 'Reps pass Freedom of Information Bill' <[http://234next.com/csp/cms/sites/Next/News/National/5679987-146/a\\_bill\\_long\\_journal](http://234next.com/csp/cms/sites/Next/News/National/5679987-146/a_bill_long_journal)>. Accessed 03.03.2011)

PARP (2010) 10 years of law making in Nigeria, Abuja. 7

Public Complaint Commission Act, Cap 37, Laws of the Federation of Nigeria, 2004

Public Service Rules, 2006 Timbuktu Media (2011) 'A bill's long journey' <<http://234next.com/cps/cms/sites/Next/News/Natioanl/5679987-146/9-bills-long-journey>>. Accessed /3/19/2011).



# **HADOPI 1 & 2: analysis and evaluation**

---

---

**Eleni Metaxa**

---

---

After turbulent legal procedures and crucial political controversies, the French legal framework for online copyright infringement was finally voted on June 12 and October 28, 2009 accordingly. The Law on “Creation and Internet” and the “Law for the Protection under Criminal Law of Artistic and Literary Works on the Internet”, with the distinctive names of Laws “Hadopi 1 and 2”, acronym of the public authority which ensures their enforcement, provide penal sanctions concerning the regulation and control of the internet access in order to decrease online piracy.

After presenting the legislative history of the Hadopi Laws, we will elaborate on the role and competences of the independent public authority and then analyze the core notions that impose surveillance on French Internet users. Then we will consider, based on the results of scientific surveys, some of the Laws’ deficiencies and the dubious effect of their repressive measures on the French Internet users’ practices.

Finally, we will raise the question of how the liberty of communication of ideas and of thought, in the form of Internet access as a political freedom, can be combined with the rights of intellectual property.

## **2. Legislative Background**

The legislative source of the Hadopi Laws resides in the European Copyright Directive of 2001, implemented in the French legal system by the Dadvsi Law voted on August 2006 but never fully put into action.

## **3. The HADOPI Authority**

The role of the independent public authority could be analyzed as follows and is summarized in the three-fold of prevention, punishment and observation of the copyright infringement.

## **4. The Graduated Response or the Three-Strike Procedure**

**4.1.** The new French copyright legislation is completed with the graduated response mechanism, a hybrid procedure divided in two distinct phases; the first conducted by the Hadopi Authority and the second by the Penal Courts.

In a first place, the collective rights organizations, the National Cinematography Center or the Public Prosecutor via their affiant agents send a report to the HADOPI with the IP addresses of the users suspected to illegally download online artistic content. In two months time, the Rights Protection Committee has to check the accuracy of the data, seek the ISPs in order to match the IP addresses to the subscribers and proceed to the first stage of the procedure. Then, an e-mail notification is sent to the subscriber informing him/her of the failure to monitor his/her internet connection, the means that protect internet access and the legal online content available.

The second phase starts six months following the first notification, on condition that a repeated offence has been committed by the same subscriber. The Authority re-sends the same e-mail message along with a certified letter of the same content stating the facts.

In the final stage of the graduated response procedure, the file is transmitted to the Prosecutor's Office. Henceforth, the criminal justice is informed about all the facts that can constitute an offence and two procedures are then possible either to prosecute the offender for copyright infringement or for breaching the obligation to monitor his/her internet access.

### ***4.2 The notice recipient's rights***

The internet user can submit his/her remarks to the Authority but cannot be informed about the artistic works claimed to be downloaded.

On the second phase of the three-strike procedure, the subscriber has finally the right to negotiate with the Authority. The person is summoned by it, informed about his/her right to be heard and, in that case he/she will be re-summoned by letter in order to proceed to the official hearing.

### ***4.3 The automatic processing of the personal data***

Additionally, in order to accelerate the judicial initiation, the personal data processing is automated leading to its massive management.

## **5. The legal online content offer**

The Authority is also charged with the duty to enforce the diffusion and the appeal of authentic artistic content legally existing on the Internet, in other words, the legal online content offer. The crucial element for the distinction of an offer as legal or not, is the permission acquired by the rights-holders to make their works available to the public. This is mainly put into practice through the reference internet portal, the music card and the Hadopi labelled websites.

### ***5.1. The reference internet portal***

The reference internet portal will be an online communication service containing all the legal offers existing for accessing an artistic work on the Web. In the form of an extended web search engine controlled by the Authority, it will identify them and assist internet users during their purchase.

### ***5.2 The «Music Card»***

As regards music, the French Ministry of Culture and Communication jointly with retailers and the National Syndicate of Phonographic Edition has put into work the service of a government subsidized card, called the «Music Card».

### ***5.3 The Hadopi labelled websites***

Finally, based on the above procedure, the Authority can grant its certification, in a form of a Hadopi logo, to websites that legally provide artistic content through public electronic communication networks.

## **6. Securing Internet Access**

### ***6.1 A new obligation to internet users***

The internet users are now responsible for monitoring their internet access for fraudulent use that can lead to reproducing, communicating to the public or making copyrighted content available. If they have successfully proceeded to that, they will be exonerated against any allegations of failure to control, in case someone hijacks their connection.

### ***5.2 Software evaluation and labellisation by the Hadopi Authority***

The Authority will grant once more its certification, in the form of a label, to different kinds of software that secure the internet access by blocking file-sharing that infringes the copyright of artistic works. The application file submitted must

contain elements proving that the specific means of security fully complies with the functional specifications validated by the Authority.

## **7. The crimes committed**

### ***7.1. Copyright infringement via online communications***

Regarding the crimes committed, the classic offence of copyright infringement is approached in the Hadopi Laws in a different way, as it is now effectuated through public online communication means, namely, the transmission of digital data which takes place via all electronic communication process.

### ***7.2 The characterized negligence; a newly born offense***

On the other hand, the person who has received the Authority's recommendations and hasn't yet installed a method to secure his/her internet access can be prosecuted for the offence of the "characterised negligence".

If the facts constitute the offence, the file is forwarded to the Prosecutor's Office and then the *Tribunal de la Police* pronounces the penalties.

### ***7.3 The additional penalty of suspending internet access***

Undoubtedly, a major implication of the graduated response mechanism is the additional penalty of internet access suspension. As described above, it is imposed not only in the case of copyright infringement, but also in the case of the characterized negligence offence.

Basing the penalty on the grounds of infringement

Internet users alleged for copyright infringement perpetrated through public online communication services may be punished with the suspension of their internet connection for maximum one year. They are prohibited to proceed to signing another internet services contract, whereas they must continue paying their subscription until its termination.

Basing the penalty on the grounds of characterised negligence

On a misdemeanour basis, the internet access of a subscriber guilty of committing a 5<sup>th</sup> class offence can be suspended for a maximum period of one month.

The obligation of the ISP to cut off the internet access

Another measure which serves as a safety valve for the efficacy of the implementation of the additional penalty is the ISP's obligation to comply within 15 days with the orders of the Court and suspend the internet connection in question.

## 8. Critical Appraisal

### 8.1. *The text of the law*

Resulting from two laws and several implementation decrees, the French system introduced against the illegal downloading of cultural works via peer-to-peer networks seems to be rather complicated, costly and difficult to put into practice.

#### **The accumulation of penalties**

As already mentioned, the penalty of suspending the subscriber's internet access can be pronounced either on the misdemeanour basis or on the grounds of copyright infringement. This not only creates the possibility of the accumulation of penalties but also several procedural issues. Finally, the criminal system proposed by the Hadopi Laws also includes two other offences: the breach of the obligation to sign during the suspension period a contract with another ISP, and the ISP's breach of the obligation to actually suspend the "guilty" internet connection after being notified.

#### **The presumption of innocence**

Despite the fact that parts of the Hadopi Law were censored as unconstitutional, some elements still raise questions about the presumption of innocence.

In case of hacking, despite the technical measures installation, the subscriber must prove that he/she has not deactivated his/her protection software and he/she has been victimized, which obviously reverses the burden of proof.

Additionally, the Authority's statements presented before the Court are principally constituted by IP addresses deprived of substantial legal proving power. Nevertheless, they are regarded as evidence forcing the alleged offender to prove his/her innocence. This can be mostly considered as a "presumption of guilt", breaching fundamental democratic principle.

#### **The suspension of internet connection**

The *Conseil Constitutionnel* considers the right to have internet access as a freedom of communication and thought. However, the alleged offender can be sentenced with its suspension for a maximum one year period. Consequently, the punishment of a 5<sup>th</sup> class offence can lead according to the Hadopi Laws to the repression of a fundamental democratic freedom, leaving the question of the respect of the proportionality and necessity of penalties yet to be answered.

Not to mention that the convicted copyright infringer must continue paying the monthly subscription fees for a service no longer offered to him/her, which can

be regarded as a “double penalty”, once again contrary to the fundamental democratic principle.

Furthermore, there has been no exemption from this penalty concerning the internet connection of companies, universities, local authorities and other organisations.

### **The ISPs’ participation**

Even though the tasks and duties delegated to the ISP companies demand a high cost of operation for the numerous devices and computers as well as the staff’s working hours, there is no legal provision for their reimbursement.

### **Technical deficiencies**

Finally, as the Hadopi Laws fight online piracy effectuated exclusively via the peer-to-peer networks, they leave outside their repressive scope, the widespread practices of streaming and direct downloading. However, since it is rapidly evolving it will soon render these Laws obsolete, not to mention the transformations of the peer-to-peer protocol and the technological means for circumventing the Laws.

## ***8.2 The results of the Hadopi 1&2 Laws application***

In this section, the result of two important surveys on the use and the expansion of the illegal downloading in France. The first demonstrated that internet users not only hadn’t stopped downloading cultural works online after the Laws’ implementation but they had opted for alternative methods, such as streaming or direct downloading, boosting that way the digital piracy. Additionally, many online buyers of cultural works are the same people who download them illegally from the websites and their internet connection suspension could lead to the eventual withering of the French cultural content market.

The second survey proved that the use of the direct download website “Megapload” had increased 20 times on November 2010 compared to that of 2008.

## **Conclusions**

To sum up, the 2009 Hadopi Laws were introduced with the aim of fighting online sharing of cultural works by means of internet access control as well as encouraging the legal online content offer in France.

They set up the “graduated response”, created the crime of the “characterized negligence” and ultimately, initiated the pronouncement of the additional penalty of the internet connection suspension.

Nevertheless, not only does the connection between the illegal downloading and the economic loss of the entertainment industry remain to be discovered but also the equilibrium between the rights of the intellectual property protection and those of the access to information should be revised. Additionally, last March the Loppsi 2 Law was voted, allowing the internet filtering without a Court decision, and also the blacklisting and monitoring of the filtered sites by an administrative state controlled authority.

Our suggestion, aligned with the proposals already expressed in France by collective organisations, would be the “global license”. This legalises the non-commercial cultural content file sharing with a fair flat-fee allocated to the rights holders, proportional to the downloading of their works. Thus, this alternative solution can be regarded as probably more effective, less repressive of the democratic fundamental rights and freedoms and more profitable to the artists.

# Social networking and the employment relationship

---

---

Stathis Mihos

---

---

## 1. Introduction

### 1.1 Aims & definitions

The aim of this paper is to examine the legal aspects of the use of social networking in relation to the employment relationship.

The term 'Social Networking' is taken to mean, as per the definition of D.M.Boyd and N.B.Ellison<sup>1</sup>, web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, view and traverse their list of connections and those made by others within the system; to the above definition the ability to exchange data with other system users in the form of comments, files, messages etc should be added, as an essential part of the services.

An 'Employment Relationship' in this paper refers to any dependent employment relationship, valid or not, for a definite or indefinite period of time, full or part-time, in any place (including home or teleworkers), irrespective of duties or tasks or position assigned.

Although the Internet and most web services are inherently world reaching, references in this paper to specific legislation will be, unless otherwise stated, to Greek legislation.

### 1.2 A networked world

Less than a year ago, the 'Economist'<sup>2</sup> suggested that if Facebook were to be a country, the ubiquitous social networking site would be the world's third most populated country with more than 500 million active users and rising fast, behind leaders China (1.35 billion) and India (1.21 billion). Myspace would be the 5<sup>th</sup> largest country with 300 million users and Twitter the 8<sup>th</sup> with 124 million.

---

1. Danah Boyd, Nicole Ellison, 'Social network sites: definition, history, scholarship', Journal of Computer Mediated Communication, Vol. 13, issue 1, pp. 210-230, October 2008, available at <<http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>> accessed 23.6.2011.

2. 'The Economist', 22.7.2010.



In fact 'Facebook' is, at the time this paper was concluded, about to reach 700 million users, according to Socialbakers<sup>3</sup>, a blog that tracks Facebook statistics.

### ***1.3 The main conflict: Public vs Private***

As with many questions relating to the use of technology in recent years, we attempt to find an analogy with the off-line world. In this context it might be fair to ask: 'If postings in cyberspace are equivalent to the behaviour in the public square, then are postings in social networks equivalent to behaviour in a private party?' Does this mean that a different set of rules apply to Social Networks, as opposed to the rules that apply to the Internet in general?

## **2. Use of social networks in an employment context**

### ***2.1 Employers and social networks: A love and hate relationship***

For businesses, the use of Social Networks is a double-edged sword, as it can have both favourable and unfavourable consequences. On the one hand social networking is a great way to:

- Create brand awareness
- Manage online reputation
- Recruit talent
- Learn about technologies and competitors
- Intercept potential prospects

On the other hand, the use of social networks gives rise to a lot of worries for employers:

- Liability (given that accusations for libel, defamation, harassment or sexual harassment, discrimination etc. based on the behaviour of the employer or of the employees in the social networks are not uncommon)
- Security issues (i.e. the 2008 Koobface worm - the name is an anagram of the word 'Facebook'<sup>4</sup>)
- Leaking of trade secrets

---

3. Socialbakers, 'Facebook is globally closing in to 700 million users!' available at <http://www.socialbakers.com/blog/171-facebook-is-globally-closing-in-to-700-million-users/> accessed 7.6.2011.

4. Lynn Greiner, 'Social networking's security pitfalls: how you can go oh so wrong with facebook, linkedIn and MySpace', 9.2.2009, available at <[http://www.cio.com/article/480030/Social\\_Networking\\_s\\_Security\\_Pitfalls\\_How\\_You\\_Can\\_Go\\_Oh\\_So\\_Wrong\\_with\\_Facebook\\_LinkedIn\\_and\\_MySpace](http://www.cio.com/article/480030/Social_Networking_s_Security_Pitfalls_How_You_Can_Go_Oh_So_Wrong_with_Facebook_LinkedIn_and_MySpace)> accessed 23.6.2011.

- Decrease in productivity (not an unfounded worry since it is estimated<sup>5</sup> that on Social Networking is spent worldwide a 22% of the total internet hours spent by all users)
- Copyright or trademark infringement
- Unauthorized use of client names or other info
- Creation of an unproductive workplace environment
- Corporate espionage. The threat is real as hackers bypass security and access sensitive data using social engineering, thus having access to lists of employees, qualifications, functions and connections and committing crimes such as loss of corporate IP, hacking networks or blackmailing employees<sup>6</sup>.

## ***2.2 Social networks misuse and the impact for the employees***

A cornerstone of employment law is the employee's obligation of loyalty to the employer<sup>7</sup> (as foreseen by articles 288, 361, 652 of the Civil Code). In essence, the obligation of loyalty means that an employee should support and not harm the lawful interests of the employer.

From the general principle of the obligation of loyalty stem specific obligations, such as the ones:

- to respect employer's personality
- to maintain confidentiality
- not to compete with employer's business
- to get along with colleagues
- not to disparage employer's products

This does not mean however, that an employee may not act against the employer's rights in order to protect her own lawful interests or expose unlawful con-

---

5. Nielsen Wire, 'Social networks/blogs now account for one in every four and a half minutes online', 15.6.2010, available at <<http://blog.nielsen.com/nielsenwire/global/social-media-accounts-for-22-percent-of-time-online>> accessed 23.6.2011.

6. To deal with these problems it is recommended by ENISA (the European Network and Information Security Agency) that employers have awareness training, security policy for Social Networks and limited provision of information. See ENISA's Position Paper 1, 'Security Issues and recommendations for online social networks', October 2007, available at <[http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks/at\\_download/fullReport](http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks/at_download/fullReport)> accessed 24.6.2011.

7. More on this at Stylianos Vlastos, 'Atomiko ergatiko dikaio' ('Individual labour law', in Greek), Ant. N. Sakkoulas Publishers, 1999.

duct (applicable also when employee's duties include postings in social networks about employers products).

It goes without saying that, absent exceptional circumstances, any misuse of the social networks by the employee, of the kind described in 2.1. above, may constitute violations of the employment contract's obligations for the employee and may be sanctioned, even leading to termination of the employment relationship.

They could also lead to penal sanctions: i.e. an employee that disseminates false or true (but confidential) information about the company could face criminal liability based on one or more of the following Penal Code provisions: Defamation (362 PC), Aggravated Defamation (363 PC), Defamation of a Corporation (SA) (364 PC), Fraud (386 PC), Fraudulent damage (389 PC), Secrecy of Letters (370 PC), Secrecy of data of particular types (i.e confidential professional or belonging to private enterprises data) (370B PC), Breach of professional confidentiality (371 PC).

It should also be reminded that a criminal act of an employee that is related to the employment relationship, may lead to unpaid termination of the employment relationship.

### ***2.3 Examples of problems in using social networks in employment or quasi employment relationships***

A significant (and growing) number of incidents involving misuse of social networks and creating tensions between employers and employees has been recorded in recent years in many parts of the world. A selection illustrating the materialization of various fears that were previously mentioned follows:

#### **Ireland<sup>8</sup>**

In 2007 a customer brought to the attention of a retail outlet that an employee had posted on Bebo unflattering comments about a manager. The employer initiated disciplinary proceedings against the employee. A disciplinary meeting was held and the employee was dismissed for gross misconduct.

The claimant initiated unfair dismissal proceedings. The Employment Appeal Tribunal held that the dismissal was disproportionate to the offence and directed that the retail outlet pay the claimant €4,000 in compensation. (*Emma Kieran v A Wear Ltd, Employment Appeals Tribunal, Case Reference UD643/2007, MN508/2007*)

---

8. As reported on Collier Broderick site, 'Dismissal judged unfair', available at <<http://www.collierbroderick.ie/Articles/Dismissal-Kiernan-v-Awear-Ltd>>, accessed 24.6.2011.

## France<sup>9</sup>

Three employees of a French consulting company, posted comments in late 2008 from their personal home computers on Facebook about company managers, including its Human Resources Director. The conversation appeared on one of the three employees Facebook page, with comments by two other employees. The employer discharged all three employees for rebellion against the company's hierarchy, and denigration of the company's image.

The employee on whose Facebook page the comments appeared chose mediation while the other two filed a complaint before the labour court.

The employees argued that the Facebook page was private and the comments were humorous. The employer argued that the list of Facebook 'friends of friends' included the employee who owned the Facebook page and other company employees and the Facebook page was capable of being read by people outside the company during the time period in which it had been posted.

The Court accepted the employer's arguments and upheld the discharge of the two employees (*Barbera v. Société Alten SIR*; *Southiphong v. Alten Société SIR*, *Prud'hommes de Boulogne-Billancourt*, Nos. RG-F-/326/343, November 19, 2010)

## Greece

In 2008 a higher education professor posted on Facebook derogatory comments as well as documents relating to the work and career of a colleague. Both professors were candidates for the same academic position.

The Court of First Instance of Thessaloniki (16790/2009)<sup>10</sup> found that the postings constituted an unlawful infringement on the claimant's personality and issued an injunction requiring the offender to refrain from using the claimant's personal data or using the Internet for the publication of the aforementioned documents.

In 2009 an airline employee was fired from her job because she was spending too much time visiting social networks such as Facebook at work, neglecting her duties and business clients calling. The employer had previously sent an email to all employees forbidding visits to social network sites.

---

9. Available (in French) at <[http://legalis.net/spip.php?page=breves-article&id\\_article=3027](http://legalis.net/spip.php?page=breves-article&id_article=3027)> accessed 24.6.2011.

10. DIMEE ('Dikaio Meson Enimerosis kai Epikoinonias' - 'Media & Communication Law', in Greek) 2009, p. 400.

The Labour Disputes Section of the Court of First Instance of Athens (34/2011)<sup>11</sup>, in a decision widely published in the Press, found that the dismissal was not abusive, as the claimant's behaviour constituted a breach of her employment contract's obligations.

### Canada<sup>12</sup>

In 2010 two employees posted on Facebook offensive comments about their supervisors and their employer. A supervisor who was an employee's Facebook 'friend' saw the comments and after being removed from the 'friends' list monitored the comments with the help of a former employee 'friend'. One of the employees alleged that his Facebook account could have been hacked as he had left it logged on at work. The employer terminated the employment of the two employees. The Union filed an unfair labour practice complaint alleging that there was no cause for termination and the employer was motivated by anti-union animus.

On 22.10.2010 the British Columbia Labour Relations Board decision in *Lougheed Imports Ltd (West Coast Mazda) v United Food and Commercial Workers International Union, Local 1518* dismissed the Union's application.

The decision established that employees have no reasonable expectation of privacy in comments made on social networking sites, and that when those comments are damaging to the employer's business or offensive, insulting and disrespectful to supervisors, the employer may have just cause for termination; however, employers should be cautious when deciding to monitor these sites.

### United Kingdom<sup>13</sup>

In 2010 a government department employee, had made several posts on Twitter mentioning the fact that she had been hungover while at work, as well as making personal comments about people she had worked with. Two national newspapers reprinted these comments in articles about the views and behavior of public officials.

---

11. Available (in Greek) at <[http://www.dsanet.gr/Epikairothta/Nomologia/mprath34\\_2011.htm](http://www.dsanet.gr/Epikairothta/Nomologia/mprath34_2011.htm)> accessed 24.6.2011.

12. The decision is available at the Labour Relations Board - British Columbia site at <[http://www.lrb.bc.ca/decisions/B190\\$2010.pdf](http://www.lrb.bc.ca/decisions/B190$2010.pdf)> accessed 24.6.2011.

13. The rulings are available at the Press Complaints Commission site at <<http://www.pcc.org.uk/news/index.html?article=NjkzNQ>> and <<http://www.pcc.org.uk/news/index.html?article=NjkzNA>> (Regarding the complaints against 'The Independent on Sunday' and 'Daily Mail', respectively) accessed 24.6.2011.

The employee complained to the Press Complaints Commission, that it was a breach of her privacy to reproduce the comments without permission

According to the commission, the employee made two main points: that it was reasonable to expect the message would only be seen by the 700 followers on her account; and that her account was clearly labeled as a personal view that did not reflect her employer's views (but not at the time the newspapers used the material)

The commission ruled to reject the complaint stating that anyone could have stumbled across the information and the retweet feature of Twitter meant there was a strong possibility it would be seen by people other than the employee's followers.

One notable point about the case is that the two newspapers stressed that Baskerville had openly used her own name rather than posting anonymously.

### Unites States<sup>14</sup>

In 2009, a business owner stumbled upon an employee's MySpace profile saying this person was planning a two-hour lunch because her boss was out of the office.

In 2010 an employee exposed 'crucial details' on Twitter about a potential business deal with a prospective client, but the client never saw the post and the deal went through.

In 2009, an account manager of a firm posted on her Facebook profile that she had quit her job. One of the firm's largest clients, previously befriended by the employee, learned about her resignation this way and lodged a complaint.

The owner of a staffing agency in Las Vegas, said some of the independent contractors she hires seem to forget that she follows them on Twitter: *'One girl said she was out having a great time drinking and she called in sick the next morning.'*

### Israel<sup>15</sup>

Although not, strictly speaking, an 'employment' relationship, this incident, by far the most spectacular, demonstrates the threat Social Networks' misuse poses

---

14. Incidents reported by Sarah Needleman, 'Facebook, Twitter updates spell trouble in small workplace', 10.3.2010, The Wall Street Journal (online), available at <http://online.wsj.com/article/SB10001424052748703701004575113792648753382.html> accessed 23.6.2011.

15. Reported by CNN World, 'Israeli military calls off raid after soldier posts details', 3.3.2010, available at <[http://articles.cnn.com/2010-03-03/world/israel.raid.facebook\\_1\\_idf-soldier-israel-defense-forces?\\_s=PM:WORLD](http://articles.cnn.com/2010-03-03/world/israel.raid.facebook_1_idf-soldier-israel-defense-forces?_s=PM:WORLD)> accessed 23.6.2011.

to a quasi employer's operations: in March 2010 the Israeli military called off a raid on a West Bank town after a soldier posted on his Facebook profile that his combat unit was going to 'clean up' the area. The soldier was reported by his friends, court-martialed and sentenced to 10 days in prison, according to media reports.

### 3. Issues in the use of social networks before, during and after employment

#### 3.1 '*Maybe we just don't like you*'

The problems start even before an employee is hired, during the selection process. It has been the general belief that when making hiring decisions, employers can lawfully use information that the applicant voluntarily disclosed and is publicly available. The advent of social networks made it extremely easy for employers to use<sup>16</sup> information posted by the applicants themselves in order to find out whether an applicant has been involved in illegal activities, but also to discover incidents of poor work ethic, including hostile feelings about previous employer and discriminatory tendencies, to check the quality of the applicant's writing or communications skills and generally to evaluate the applicant's judgment in maintaining his or her public online persona.

However employers run the risk of being held criminally and/or administratively liable if found to have violated, in a hiring decision, anti-discrimination in the workplace laws (L.3304/2005) related to use of criteria such as race, age, disability, religion, sexual orientation etc.

Still, regulation is fast moving to claim this, so far uncharted, territory. In Finland, Data Protection Ombudsman Reijo Aarnio ruled that employers cannot use Internet search engines (i.e. Google) to obtain background information on job candidates<sup>17</sup>. In the UK the Employment Practices Code published by the UK Information Commissioner's Office says<sup>18</sup> that during a recruitment process, em-

---

16. In fact, in 2008 already 20 percent of companies admitted to checking out candidate's profiles on social-networking sites. PC World, Carrie-Ann Skinner, '*Employers Admit checking Facebook before hiring*', 14.9.2008, <[http://www.pcworld.com/businesscenter/article/151044/employers\\_admit\\_checking\\_facebook\\_before\\_hiring.html](http://www.pcworld.com/businesscenter/article/151044/employers_admit_checking_facebook_before_hiring.html)> accessed 23.6.2011.

17. Nicole Kennedy, Matt Macko, '*social networking privacy and its effects on employment opportunities*' in '*Convenient or Invasive? The Information Age*', available at <<http://www.ethicpublishing.com/inconvenientorinvasive/2CH12.pdf>> accessed 23.6.2011.

18. European Digital Rights site, '*Germany wants a new law to protect employees' privacy*', EDRight - Number 8.17, 8 September 2010 available at <<http://www.edri.org/edright/number/8.17>>

ployers have to: *'Explain the nature of and sources from which information might be obtained'*. Even more drastic, a bill<sup>19</sup>, to be passed by the German Parliament, would prohibit employers from using social networking sites such as Facebook (but not 'professional' online networks such as LinkedIn or Xing) when conducting background checks and screening current and potential employees.

### 3.2 *'To poke or not to poke at work?'*

As already mentioned, employers have many reasons to be concerned about the use of social networks at work. During the employment, the most pressing issue regarding use of social networks in the workplace is whether or not to allow it and if not how to implement such ban. The simplest solution for an employer is to limit access at such networks from the workplace, to the extent possible. Indeed, according to a survey<sup>20</sup> social networks are among the most commonly blocked websites in businesses. Here's the top ten (percentages indicate proportion of business networks using blacklisting feature that reference a given site):

1. Facebook.com — 23%
2. MySpace.com — 13%
3. YouTube.com — 11.9%
4. Ad.Doubleclick.net — 5.7%
5. Twitter.com — 4.2%
6. Hotmail.com — 2.1%
7. Orkut.com — 2.1%
8. Ad.Yieldmanager.com — 1.8%
9. Meebo.com — 1.6%
10. eBay.com — 1.6%

For businesses that want to limit their employees' access to social networks, filtering is the legally safest option, as it is less invasive than monitoring. It remains, however, an open question whether blocking employees' access yields results, since use of social networking has become the norm, especially among younger workers. TUC (British Trades Union Congress) General Secretary Brendan Barber

---

number8.17/law-facebook-germany-employees> accessed 24.6.2011.

19. Morrison & Foerster Social Media Newsletter, Vol. 1, Issue 3, p.5, September 2010, available at <<http://www.mofo.com/files/Uploads/Images/100927-Socially-Aware.pdf>> accessed 24.6.2011.

20. OpenDNS '2010 Report web content filtering and phishing'. Source: Sample of OpenDNS business networks using whitelisting in 2010 (n = 31,623) available at <<http://www.opendns.com/pdf/opendns-report-2010.pdf>> accessed 18.6.2011.



said<sup>21</sup> in 2007: *'Simply cracking down on use of new web tools like Facebook is not a sensible solution to [the] problem ... Better to invest a little time in working out sensible conduct guidelines, so that there don't need to be any nasty surprises for staff or employers.'*

### **3.3 'Gone, but not forgotten...'**

Problems relating to social networks do not end, for employers, when an employee leaves from. Supervisors and co-workers are increasingly asked to 'recommend' former employees on LinkedIn after separation from employment.

Technically, a positive recommendation on a person's LinkedIn page is not the same as an employment reference (Art. 678 Civil Code), unless given by an authorized company representative and has been requested by the employee.

However in practice it amounts to the same, so employers should consider adding to their policies a prohibition on managers from 'recommending' or commenting on the job performance of former employees via social media without prior specific authorization.

## **4. The concept of 'friendship' in social networks used in an employment context**

### **4.1 Between friends & the 'household exemption'**

An interesting question is raised when discussing comments posted on social networks: are we taking things too far? Shouldn't we tolerate comments that take place in discussion between friends, much as we do when such discussions take place in the non virtual world?

To answer this question we should consider a few issues. But first of all it is not entirely true that we have (at least legally speaking) a higher degree of tolerance for acts that violate a law, even when they take place among friends (more on that later). But the latin proverb *'verba volant, scripta manent'* obviously applies in this case, too, giving the impression that just because certain acts in the non virtual world are not documented, they are not punishable.

In any case, I suggest that an analogy applies with the *'household exemption'* introduced by the Opinion 5/2009 of the Working Party of Article 29 of Directive

---

21. Mail online, *'Let workers use Facebook during office hours, say union bosses'* available at <<http://www.dailymail.co.uk/sciencetech/article-478699/Let-workers-use-Facebook-office-hours--say-union-bosses.html>>, 30.8.2007 accessed 18.6.2011.

95/46/EC<sup>22</sup>. According to this Opinion, when users operate within a purely personal sphere, contacting people as part of the management of their personal, family or household affairs, the regulations governing data controllers do not apply. However, the '*household exemption*' does not apply and the user might be considered to have taken on some of the responsibilities of a data controller, if a user:

- acts on behalf of a company or association
- uses the social network mainly as a platform to advance commercial, political or charitable goals
- acquires a high number of third party contacts, some of whom he may not actually know
- takes an informed decision to extend access beyond self-selected 'friends'
- provides access to profile to all members within the social network or the data is indexable by search engines

The number of third party contacts ('friends') is indeed a strong indication of the type of use. Dunbar's Law (Robin Dunbar, British anthropologist): limits<sup>23</sup> to 150 the number of individuals with whom any one person can maintain stable relationships. Facebook allows a maximum of 5,000 connections. BT's innovation head JP Rangaswami<sup>24</sup> thinks (but has not proved) that social software might help raise the Dunbar number.

Given the above, I am inclined to suggest that if the household exemption does not apply, then we are *not* in a closed environment of friends.

It should also be noted, as was mentioned earlier, that even the application of the household exemption does not exclude the possibility of a user being liable according to general provisions of national civil or criminal laws in question (e.g. defamation, liability in tort for violation of personality, penal liability).

#### ***4.2 When a 'friend' is not a friend***

In most social networks, the user has a degree of control over the privacy settings. He or she can limit access to his or her information, thereby excluding people that can potentially harm the user. Employers or potential employers would of-

---

22. Adopted on 12 June 2009 available at <[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf)> accessed 18.6.2011.

23. Research Intelligence, The University of Liverpool, Issue 17, August 2003, p.3, available at <<http://www.liv.ac.uk/researchintelligence/issue17/pdf/resint17.pdf>> accessed 18.6.2011.

24. '*Of followers and followees and friends*' available at <<http://confusedofcalcutta.com/2009/01/11/of-followers-and-followees-and-friends/>> accessed 18.6.2011.

ten fall into this category. What then if they try to bypass the restrictions imposed by a user? Can one have access to information posted on social sites by *deceptively* 'friending' a person? (i.e. the employer befriending an employee by not revealing his or her real identity).

It is more than likely that such an action would be illegal, although it is not entirely clear which article of the Penal Code would be breached (Article 386 PC refers to fraud, but requires damage to property which would be hard to prove, 370C par.2 PC or 22 par. 4 L.2472/1997 forbid unauthorized access to data, but the concept of 'authorization' might constitute an issue when user does grant access and 415 PC, a misdemeanor, punishes the unauthorized change of name). In all cases, an employer that would use data that have not been collected fairly and lawfully, as article 4 of L.2472/1997 requires, risks being subject to the administrative, civil and possibly criminal sanctions that the Law foresees.

When, however, the *real* name is used, an ethical issue might arise but not necessarily a legal one (with the exception of Lawyers, who, collecting data in such a manner possibly violate article 38 of the Code of Ethics)<sup>25</sup>.

## 5. Conclusions

Social networks developed rather recently, as part of what is now commonly called Web 2.0. The law, certainly moving in slower speed than technological developments, has not yet dealt specifically with the issues arising from social networks (mis)use, in general or, more specifically, in the employment relationship. This does not mean that their use is not regulated. As is to be expected, courts apply general principles and legislation in matters involving social networks that are brought before them. However, the employment relationship, by its nature sensitive and dynamic, flourishes and bears fruits when the rules that govern it are clear, precise and respected. To this end it is recommended that employers

---

25. "A lawyer has the obligation to avoid any communications with the opponent and any discussion related to the case, without his client's approval. If the opponent has hired a lawyer for the case, his lawyer should be called in all discussions... A lawyer should not act in a malicious manner to cause the loss of rights by his opponent...". It is interesting to note that the New York State Bar Association and the New York City Bar Association have issued opinions on whether a lawyer may or may not "friend" an individual to obtain information. When the lawyer's real name is used, Rule of Professional Conduct 4.2, which prohibits a lawyer from communicating with a represented party about the subject of the representation absent prior consent from the represented party's lawyer, is applicable (Paul Garrity and Kathryn Hines, '*Legal ethics and the social network*', 18.10.2010, available at <<http://www.social-medialawupdate.com/2010/10/articles/ediscovery/legal-ethics-and-the-social-network/>> accessed 23.6.2011).

have in place a risk mitigation policy and program. This may sound commonplace, however a survey showed that only 17% of employers actually do have such a policy. (Deloitte 2009<sup>26</sup>)

The employer may use the policy in addition to other company policies, to specifically address issues relating to Social Networks, such as to<sup>27</sup>:

- Prohibit the use of *company email address* to register with a social network
- Prohibit the use of company *logos or trademarks* in postings, pages etc.
- Request employees to *disclose* (to identify themselves as employees of the company, if needed, as in cases when they write reviews for company products) and *disclaim* (that the views express are those of the employee and do not reflect the views of the employer)
- Prohibit *tweeting* during company meetings.
- Give *guidelines* on friend requests by colleagues or managers and
- Generally *regulate*, to the extent that this does not contradict the Law, the Social Networks use by the employees.

A policy should not try to set out all forms of Social Networks, as it would run the risk of being outdated by the time it was adopted.

## 6. Future Research

This brief analysis of the matter has not been concerned, for lack of time and resources, with the important issue of trade union rights in using social networks. This may well be a sub-chapter in the greater issue of trade unions' use of the Internet, but given the rise in use of the social networks, I believe that further discussion is needed on whether and how archaic and quickly turning to obsolete methods of trade union communications can be adapted to the Internet age without disrupting the essential workplace order.

---

26. Elizabeth McNamee, Kim Magyar, 'Are you building a house of cards? social networking in the Office', ACC Docket, Vol. 28, issue 7, pp. 29-38, September 2010.

27. Useful suggestions can be found in Larry Silverman and Terri Imbarlina Patak's article 'How you can safely use social media with employees', ACC Docket, Vol. 28, issue 3, pp. 19-30, April 2010.

# **Personal financial data in danger: the case of the new smart tax-card in Greece**

---

**Milossi Maria &  
Alexandropoulou Evgenia**

---

## **1. Introduction**

Personal financial data is an important category in personal data, as it reflects the individual's economic behaviour and financial status. On a daily basis, personal financial data is a necessary tool for those who are legally authorized as processors, not only in the field of enterprise but also in the field of public service. This procedure allows the processors to obtain important information concerning the individual's credit status, including insolvency risk, tax status, allowances and special financial privileges (Milossi & Alexandropoulou-Egyptiadou, 2010).

The legal framework regulating the protection of personal financial data is found in a) Directive 95/46/EC on "the protection of individuals with regard to the processing of personal data and the free movement of such data" and b) Law 2472/1997 (Official Gazette, A' 50/10.4.1997) on the "Protection of Individuals with regard to the Processing of Personal Data", through which the above-mentioned Directive has been implemented in Greek Law (Avgoustianakis, 2001, Armamentos & Sotiropoulos, 2005). According to article 8 of the Directive, personal financial data is considered to belong to the category known as simple data and not as sensitive data, despite the fact that financial data refers to a strictly private sector of an individual's life (Igglezakis, 2003).

## **2. Enforcement of tax policy as provided by L. 3842/2010 and the related dangers to personal data**

By passing Law 3842/2010 (Official Gazette, A' 58/23.04.2010) concerning the establishment of taxation justice, the Greek government aimed to decisively reinforce its tax policy, thus meeting the needs for flexible public services (Milossi & Alexandropoulou-Egyptiadou, 2011, Milossi & Bozinis, 2010), saving on costs and reducing bureaucracy. One of the first steps in this direction is art. 1, according to which tax-payers must collect receipts for their transactions in order to qualify for tax-allowances. The government's main target is to establish taxation justice, by more efficiently controlling taxpayers' transactions and considerably reducing tax evasion. In the context of the above regulation aiming to aid the

taxpayer in the collection of receipts, the Greek government has introduced an e-registration system based on the use of a smart tax-card.

However, this system poses challenges and risks infringements of individuals' privacy (Mitrou, 2001, Gerontas, 2002). With this in mind, the General Secretariat of Information Systems (GSIS) of the Ministry of Finance asked the National Data Protection Authority (DPA) to state an opinion on the abovementioned e-registration system. Recently, the DPA has provided its opinion.

### **3. Brief description of the e-registration system in question**

According to the G.S.I.S., this system is based on the banks' already existing infrastructure for credit or debit card transaction processing (Sinanioti-Mavroudi & Farsarotas, 2005). This infrastructure consists of POS (points of sale) or any other bank infrastructure which is aimed at processing retail transactions.

Under supervision of the Ministry of Finance, the banks will issue smart cards containing a magnetic strip with a personalized unique 19 digit number. To protect the card holder's privacy, the issuing bank shall not retain the cardholder's personal data, thus making identification impossible. Citizens are entitled to more than one card for themselves and members of their family. Each card will have a unique card number but all will be related to the same tax number. Once receiving the card, the cardholder is obliged to declare his card number/s to the GSIS, via an e-mail or an SMS.

During a POS transaction, the card will register the amount of the receipt or the equivalent amount of debits and then the transaction will be sent to the issuing bank for processing. Each bank is then responsible for sending a file containing the cardholder's card code, the enterprise's tax number, the time and date, as well as the amount of the transaction (or the equivalent debits) to the GSIS.

Taking into consideration that a citizen may hold more than one tax card related to his/her tax number, the G.S.I.S. will accumulate all transactions using any of these cards. Every cardholder will have access to his receipt file, kept by GSIS, by entering his personal account in the General Secretariat's portal.

At the end of each financial year, the GSIS will accumulate each cardholder/taxpayer's receipts for two reasons: a) to provide the necessary tax allowances to the taxpayers and b) to assure VAT collection and return. The tax payer has, from the time he is informed of the final sum for that financial year, to appeal against the accuracy of his receipt file in a period that will be defined by G.S.I.S. exercising his right to be informed (Tountopoulos, 1999). In a month after the end of this period all transaction details will be erased (right to oblivion) (Fenoll-Trousseau & Haas, 2000), save the final sum of the receipts for the year.

According to the G.S.I.S's opinion, a card's anonymity makes the cardholder's identification impossible to third persons (including the issuing bank). In fact, only the GSIS is permitted to identify the cardholder/taxpayer. Moreover, a cardholder consumption profile cannot be created, due to the fact that the e-registration system will contain only the total amounts with no reference to the purchased products or services.

#### **4. DPA's opinion 4/2010 on the new tax smart card**

According to article 19 of Law 2472/1997 and 28 of 95/46/EC directive, the DPA has the power to state opinions which implement rules regarding the processing and protection of personal data, as well as to examine controllers inquiries concerning the legitimacy of data processing. In the case of the smart tax card, the DPA has stated that article 9 of Law 2238/1994 and article 1 of Law 3842/2010, which allow for tax allowances from the receipt collection, do not provide adequate legal ground for the above mentioned e-registration system; the reason for this being that with the e-registration system, data is more exposed to infringement of privacy.

Thus, it is necessary to have a new and specific regulation system for the e-registration process. The new regulation system must also provide for: a) an optional character to the specific e-registration system, b) controllers' obligation to inform the data subject on the purpose of the processing, the type of data, the recipients and the controller's details, c) data subjects' explicit and specific consent (art. 2 k, L. 2472/1997), d) card holders' details being identified only by the GSIS, in order to avoid a consumer profile, which could be created by combining data from the credit card and the smart tax card.

Additionally, the DPA, taking into consideration that the new e-registration system's main purpose is to facilitate tax payers with their tax declaration, including their tax allowances, as well as to control enterprises VAT returns, has suggested that: a) an individual's identification must be protected and only disclosed during the process of tax declaration; this suggestion is covered by article 4 of Law 2472/1997, according to which "data is kept in a form which permits the identification of data subjects for no longer than the period required, and for the purposes for which such data was collected or processed" and b) concerning VAT returns, an individual's identification is not necessary while the data transfer is taking place in real time.

More specifically, the DPA has suggested the need for a more appropriate infrastructure to register taxpayers' expenses. This proposal is based on the use of an alternative, strictly confidential to its holder smart card, which will allow him to upload its contents. As for an enterprise's on line connection, a measure which

could effectively control VAT returns is the cash register's on line connection directly to the Ministry of Finance. Thus, an enterprise's transactions will be registered automatically to the Ministry's database and the file created will not contain any customer personal data. As this data is not necessary for the abovementioned purpose, this e-registration system guarantees a citizen's anonymity, eliminates customer profile creation and makes VAT returns control more efficient.

Recently, the Greek Government has passed Law 3943/2011 (Official Gazette, A'66/31.03.2011) on «fighting fraud, staffing audit and other provisions concerning the Ministry of Finance» which, explains in detail the e- system supporting the new smart tax card.

## 5. Conclusions and final thoughts

Thus, to implement taxation justice provided by Law 3842/2010, the GSIS has suggested an alternative receipt e-registration system. This system aims to facilitate taxpayer declaration, including tax allowances, and to more efficiently control VAT returns. However, this suggestion has met with strong objections from the DPA, due to the danger of infringement of personal data.

According to the DPA, the need for an appropriate infrastructure to support the use of a smart tax card has to be combined with respect for personal data processing principles and related technological safety regulations.

In order to verify whether data is lawfully processed by means of the abovementioned smart tax card, the “three step test” is proposed (Alexandropoulou, 2007). STEP 1: The examination of whether the processing principles have been applied. These are the principle of purpose, of proportionality, of accuracy and of a pre-determined storage time. In cases where these principles have not been applied during the data's processing, the processing becomes illegal and any further examination ceases. In cases where all principles are applied, step 2 follows. STEP 2: Data subject consent is required. Consent must be granted according to the conditions provided by Law, thus making the data processing legal. Where data subject consent does not exist according to the Law, step 3 follows. STEP 3: The search concentrates on whether in the case in question consent is not required. In such cases the processing becomes legal.

Finally, the smart tax card being optional, presupposes that if a data subject consents to its use, he/she is in effect giving consent according to the law (step 2). The DPA's objections are whether the data processing principles are applied (step 1). Conclusively, the DPA's proposal, based on the use of an alternative, strictly confidential to its holder smart card, protects citizen personal data efficiently without inhibiting the control of enterprises VAT returns.



## References

### *A. Books and papers*

**Alexandropoulou-Egyptiadou, E. (2007):** Personal Data-The legal framework of their electronic processing, A.N. Sakkoulas Editions, Athens-Komotini. (in Greek)

**Armamentos, P. & Sotiropoulos V. (2005):** Personal Data. Interpretation of L. 2472/1997, Sakkoulas Editions, Athens-Thessaloniki (in Greek)

**Avgoustianakis, M. (2001):** Individual's protection of personal data's processing- Problems and law treatment, Human Rights, DtA (2001), V.11, A.N. Sakkoulas Editions, Athens-Komotini, page 673

**Fenoll-Trousseau, M. P. & Haas, G. (2000):** Internet et protection des données personnelles, editions Litec, Paris

**Gerontas, A. (2002):** Citizen's protection of personal data's electronic processing, A.N. Sakkoulas editions, Athens-Komotini, pages 93, 99-100

**Igglezakis, I. (2003):** Sensitive Personal Data, Sakkoulas Editions, Athens-Thessaloniki

**Milossi, M. & Alexandropoulou-Egyptiadou, E. (2010):** Protection of personal financial data: Regulatory framework of their e- processing focusing on the function of interbanking information systems in Greece and France, in An Information Law for the 21st Century Bottis M. (ed.), Nomiki Bibliothiki, page 237

**Milossi, M. & Bozinis, A. (2011):** E-government and financial development: Contemporary problems and perspectives. Case studies in Greece, proceedings of International Conference on International Business 2011, 20-21 May 2011, Thessaloniki/GREECE, (unpublished)

**Mitrou, L. (2001):** The law in information society, Law & society on the 21<sup>st</sup> century, Sakkoulas editions, Athens-Thessalonki page 34

**Sinanioti-Mavroudi, A. & Farsarotas, I. (2005):** Electronic banking, A.N. Sakkoulas editions, Athens-Komotini, pages 183 et seq.

**Tountopoulos, V. (1999):** Data subject's right to information, Enterprises' and Companies' Law, DEE (1999), V.5, Nomiki Bibliothiki, page 576 et seq. (in Greek)

### *B. Legal texts and decisions*

Law 2472/1997: Official Gazette, A '50/10.04.1997

Directive 95/46/EC: Official Journal L 281, 23.11.1995

Law 2238/1994: Official Gazette, A '151/16.09.1994

Law 3842/2010: Official Gazette, A '58/23.04.2010

Law 3943/2011: Official Gazette, A '66/31.03.2011

Ministerial Decision of Minister of Finance 1104/9-5-2011

### ***C. Sites***

Data Protection Authority: [www.dpa.gr](http://www.dpa.gr)

General Secretariat of Information Systems: [www.gsis.gr](http://www.gsis.gr)

Ministry of Finance: [www.minfin.gr/portal](http://www.minfin.gr/portal)

# E-privacy in practice

---

---

Misic Klemen

---

---

## ePrivacy in Practice

ePrivacy in Practice depends on people in most cases. Technology is capable of guarantying security, but there is always a human on the top of the security chain – administrator or super administrator. And the question who supervises the supervisors still remains unanswered. So what can we do to secure privacy in electronic world in a way to reduce the impact of the human factor?

## Privacy by design (PbD)<sup>1</sup>

Privacy by Design represents an approach whereby privacy and data protection compliance is designed within an information holding system right from the start, rather than being bolted on afterwards or maybe even ignored, as has too often been the case.

PbD is not an almighty solution for all data breaches, but it ensures a high level of privacy stability of the system. It is an added value for data security, since the legislation and regulations lag behind new technology. There is a common reflection that implementing privacy *and* security into a system leads to a zero-sum relationship. It means that in order to increase privacy you must decrease security or vice versa. However, nowadays this is not true. Sure, it requires more energy and sometimes a bit more financial resources, but at the end implementing PbD into a system is a positive-sum relationship. Here are two examples to confirm my statement:

1. Researches show that loosing 1 % of the organisation's reputation leads to loosing 3 % of the profit,
2. 2009 Annual Study: Cost of a Data Breach, Ponemon Institute, February 2009: the average cost of a data breach is about \$202 per record.

Some extra disadvantages of not implementing PbD into a system are:

- legal liabilities,
- diminished brand reputation,
- loss of costumers.

---

1. 'Privacy by Design' was originally conceived and developed by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, more than 10 years ago.

Privacy By Design is an approach advocated by Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario. She constituted some basic principles which shall be introduced into systems to achieve suitable PbD standards and avoid the consequences stated/described above. These principles<sup>2</sup> are:

- a. **Proactive not Reactive:** the main principle which differentiates this method from “old” standard methods of privacy implementing. Companies should implement PbD into its systems prior to starting the system / product production, preventing problems before they appear rather than dealing with them after they have already emerged. This can be best achieved by considering the results of an exact Privacy Impact Assessment (Risk Analysis).
- b. **Privacy the Default:** nowadays an individual has to set the privacy level manually in most systems, which can often lead to security defectiveness. Moreover, an average individual is not capable of optimizing privacy settings because he lacks the knowledge. For these reasons privacy should be set as the Default. A recent bad practice example is geolocation data collection of individuals using iPhone or Android based phones.
- c. **Privacy Embedded into Design:** Privacy should be implemented into the structure of the system or product. Privacy simply becomes a part of the system or the product.
- d. **Full Functionality:** no unnecessary trade-offs should be done to achieve a functional PbD. The system / product should keep its full functionality, privacy matter is only an added value to the product. Example: the use of biometrics cards – a template of a fingerprint is saved on an encrypted card; to enter the system one must present the card and his finger (actual fingerprint); the system compares the template stored on the card and the actual fingerprint; this way, from the system’s point of view, there is no need for the system to store any data while its functionality is not diminished and, from the individual’s point of view, the individual retains complete control over his / her biometric data.
- e. **End-to-End Security, Lifecycle Protection:** PbD should not be limited to a time limit. On the contrary, PbD should always be considered as an integral part of a system or product and the PbD efficiency level should be evaluated at least periodically if not constantly.
- f. **Visibility and Transparency:** parts of the system or product as well as separate operations within the system or product should be visible and transparent to users and providers alike. According to this principle users

---

2. See more: <http://privacybydesign.ca/>.

are able to change the system's privacy settings and adjust the system to suit their preferences and needs.

In 2010 The Information Commissioner of The Republic of Slovenia awarded the first Ambassador of Privacy prizes (orig. Ambasador zasebnost) –to controllers of personal data, who were the first to integrate the concept of PbD successfully into their products:



*Latest example (lack of PbD):*

16/5/2011:

<http://www.h-online.com/security/news/item/Android-apps-send-unencrypted-authentication-token-1243968.html>:

*“Attackers can potentially exploit an Android data transmission vulnerability to gain access to, and manipulate, other users’ Google Calendar, Picasa Web Album and Google Contact data. The issue exists because an authentication token (authToken) received when logging into the Google server is subsequently transmitted in plain text by some applications. Researchers at Ulm University in Germany report that, in unencrypted Wi-Fi networks and in networks where all users use the same Wi-Fi key, attackers can potentially use Wireshark to intercept the token and use it for their own purposes.”*

### **“Do Not Track” Mechanism**

This principle can be considered as complementary to PbD. We can say everyone is being tracked somewhere – by mobile operators, mobile phone producers (see the example with iPhone and Android above), by the state...

Some forms and means of tracking cannot be avoided – however, at least in the private sector, enabling the individual to assert his privacy rights is possible. ‘Do not track’ right can simply be described as “one-stop-shop where customers can exercise a choice not to be tracked, and where marketers would have to respect their choice<sup>3</sup>.” This definition was adopted from the field of marketing, since the majority of tracking forms and means in private sector are performed for the purpose of marketing.

In order to fully implement the right not to be tracked into a system or product controllers of personal data should consider The Federal Trade Commission’s proposal and regard the following principles<sup>4</sup>:

1. **Do Not Track mechanism must be easy for consumers to use and understand:** The Privacy Policy cannot be considered as clear and transparent if it is stated within small print, a very extensive text or is described vaguely. The consumer should know what kind of privacy settings he or she uses.
2. **Do Not track mechanism must be effective and enforceable:** the mechanism is useless and ineffective if the consumer is enabled to (de-) select solely a limited array of privacy-friendly settings.
3. **Do Not Track mechanism must be universal:** privacy settings differ from program to program, from browser to browser – it is not difficult to notice the differences between i.e. *Safari, Firefox or Chrome*. Even the most essential privacy settings options vary notably. By implementing universal settings it can be achieved that even an “average” user can identify and set them according to his own preferences. A good example of such a universal *Do not Track* mechanism can be found in some countries in the form of so called *Do not Call* registries – no matter which telephone operator provides the phone number, the procedure is the same – once an individual expresses his wish not to be disturbed for commercial purposes via the chosen phone number a *Do not Call* sign must be stated next to the phone number in any phone book where the user’s phone number is published.
4. **Do Not Track Mechanism must allow consumers to opt out not only from the use of tracked data, but also from its collection:** browsers or other systems can technically collect data in a manner that an individual does not have any influence on such processing of his personal data. If an

---

3. Definition by David C. Vladeck, Federal Trade Commission, US.

4. The principles can be found at: <http://www.ftc.gov/speeches/vladeck/110308forasspeech.pdf>.

individual is not given the lever to disable not only the use of tracked (collected) data but the option to disable the collection alone as well, such a mechanism is insufficient. This is referred to as *the function creep*<sup>5</sup> and can be considered as abuse of data collected.

- 5. Do Not Track mechanism should be persistent:** the mechanism is not fully functional if the individual has to disable the tracking every time he or she enters the system (runs the browser).

## Privacy impact assessment<sup>6</sup>

A Privacy Impact Assessment – PIA<sup>7</sup> is an identification, analysis and risk-reduction tool which may be used to avoid the illegal handling of personal data, which can occur during the implementation of any project, system or technology. Such assessments are more established in those environments where the legislative and the supervisory emphases lie on the protection of privacy and not so much on the safeguard of data protection.

PIAs are based on the systematic and timely identification of risks emanating from the illegal handling of personal data; they can be used for the early detection of risks and their easier elimination, reduction or acceptance thereof. In a way, PIAs are similar to inspections as to the legality of processing of personal data pursuant to Data Protection Law, which is conducted by the DPAs and where emphasis is placed on an assessment of compliance with Data Protection Act, whereas the purpose of the PIA is prior risk analysis, as well as optimization of procedures for achieving compliance.

The basic principles of the PIA build on the fundamental doctrine of the protection of personal data are:

- 1. Legality:** The principle of legality means that the general rules of processing personal data shall be prescribed by law. The latter is particularly germane for legal entities under private law, for which a general authorization and the general rules are for the most part predetermined by statute, while more detailed rules may be stipulated by way of the provision of the personal consent of the individual concerned, or a contract, or similar such

5. Phenomenon, where data is primarily collected for a certain purpose and then, after a time, is also used for other purposes, by other erstwhile unknown processors and users.

6. Abstract out of Slovenian IC's guidelines:  
[http://www.ip-rs.si/fileadmin/user\\_upload/Pdf/smernice/PIA\\_in\\_e-administration.pdf](http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/PIA_in_e-administration.pdf).

7. For more on the historical background and characteristics of the PIA see: <http://www.rogerclarke.com/DV/PIAHist-08.html>.

agreement. Actual designation of the processing of personal data under law is – as a rule – applicable in the public sector.

2. **Honesty and transparency:** Honesty and transparency logically refer to the fact that the processing of personal data shall be conducted in a manner which is honest and apparent to the individual. In addition to knowing by whom and under what conditions their data will be processed, each individual person must be aware as to what personal data will be processed, who will process it, and for what purposes.
3. **Proportionality:** Proportionality means that it is only permissible to collect and to process the smallest scope of personal data necessary to achieve the purpose of processing personal data. Proportionality may primarily mean that if such personal data is not necessary to achieve the goal, then it is not appropriate to collect it. Some very obvious examples of disproportionality include:
  - Requiring a personal identification number when buying milk;
  - Requiring multiple unique identifiers (e.g. personal identification number and tax number at the same time) ;
  - The collection of unnecessary data ("The on-line system would not let me continue without providing all this information" "This is our standard form", "Just complete this in full...")
4. **Accuracy and contemporaneity:** The principles of accuracy and keeping up-to-date dictates that the data being processed must be correct and current. Accuracy means that the data is not erroneous or incomplete, whereas keeping up-to-date means that the most recent data is used. Personal data may be accurate but not up-to-date, which means that data is used which is accurate and valid at a certain point in time; however, newer and more up-to-date data is also available. The frequently iterated argument '*I have got nothing to hide*' is quickly diluted if the principle of accuracy and keeping up-to-date is not respected, and your data in certain records becomes erroneous or inaccurate.
5. **Retention period:** Retention is likewise predicated upon the principle of proportionality, and thus personal data may only be stored for the period of time required to achieve the purpose for which said data has been collected and further processed. After having fulfilled the purpose of processing, personal data should be deleted, destroyed, blocked or anonymized, unless such data has been categorized as archival material under the provisions of the law regulating archival materials and archives, or it is retained under



the tenets of other legislation which mandates the retention of certain personal data.

- 6. Personal data security:** Personal data security is a narrower term than the protection of personal data, and refers to organizational and technical measures by means of which personal data is made secure; thus personal data security represents the prevention of accidental or intentional unauthorized destruction of data, its amendment or loss, as well as the unauthorized processing of data. In other words: our personal data can be exceptionally well protected under a competent data security system; this said, however, personal data is still open to abuse, particularly so if other principles are not taken into consideration (e.g. data processing without a legal basis, its application for purposes other than that which it was specifically collected, as well as the excessively long retention of data and suchlike).
- 7. Observing the rights of the individual:** One of the essential principles of personal data protection refers to the individual whose personal data is processed by an operator in the public or private sector. Any individual namely enjoys the right to familiarization with their own personal data and, in the event of established irregularities, also enjoys the right to object as well as require the amendment, correction, blockage or deletion of erroneous data.

# Public domain vigor in copyright based on John Locke

---

Marinos Papadopoulos &  
Alexandra Kaponi

---



This work is licensed under a Creative Commons Attribution-Non-Commercial-No-Derivatives v.3.0, GR license (see license at <http://creativecommons.org/licenses/by-nc-nd/3.0/gr>)

## Immanuel Kant

Immanuel Kant, who is credited with setting the foundations of intellectual property in European continental law,<sup>1</sup> writes in section 31/II of the “Metaphysics of Morals”<sup>2</sup>: “Why does unauthorized publishing, which strikes one even at first glance as unjust, still have an appearance of being rightful? Because on the one hand a book is a corporeal artifact (*opus mechanicum*) that can be reproduced (by someone in legitimate possession of a copy of it), so that there is a right to a thing with regard to it. On the other hand a book is also a mere discourse of the publisher to the public, which the publisher may not repeat publicly without having a mandate from the author to do so (*praestatio operae*), and this is a right against a person. The error consists in mistaking one of these rights for the other.”

For Immanuel Kant, the book belongs to whoever has written it and this independently from the number of exemplars of the book or of the work of art in their passages from owner to owner. The initial bond cannot change and it ensures the author authority on the work. The peculiarity of intellectual property consists

- 
1. Otfried, H., (1996), *Immanuel Kant*, 4th ed., Munich; Mulholland, L.A., and Elliott, E.J., (1990), *Kant's system of rights*, Columbia University Press; Stengel, D., (2004), *Intellectual property in philosophy*, 90 ARSP, pp. 20-50; Westphal, K.R., (2002), *A Kantian justification of possession*, in *Kant's metaphysics of ethics: interpretive essays*, Mark Timmons ed., New York, Oxford University Press, pp. 89-109; the same, (1997), *Do Kant's principles justify property or usufruct?*, *Jahrbuch für Recht und Ethik/Annual Review of Law and Ethics* 5, pp. 141-194; Byrd, S. B., and Hruschka, J., (2010), *Kant's doctrine of right, a commentary*, Oxford University Press.
  2. Kant, I., (1996), *The Cambridge edition of the works of Immanuel Kant, practical philosophy*, Cambridge University Press, Paul Guyer and Allen M. Wood eds., pp. 437-438, available at <[http://books.google.gr/books?id=0hCsbUjFiBwC&printsec=frontcover&source=gb\\_s\\_ge\\_summary\\_r&cad=0#v=onepage&q&f=false](http://books.google.gr/books?id=0hCsbUjFiBwC&printsec=frontcover&source=gb_s_ge_summary_r&cad=0#v=onepage&q&f=false)> [last check, Apr. 20, 2011].

thus first in being indeed a property but property of an action; and second in being indeed inalienable but, also, transferable in commission and license to a publisher. The bond the author has on his work confers him a moral right that is indeed a personal right, a right attached to the author's personality. It is also a right to exploit economically his work in all possible ways, a right of economic use, which is a patrimonial right. Kant argued that the moral right and the right of economic use are strictly connected and that the offense to one implies inevitably offense to the other.<sup>3</sup>

In his essay titled "*On the Illegitimacy of Print Piracy*", Kant asserts the presence of a direct link between the author and the reader of an author's book in the sense that through book the author speaks directly to the readers, thus the ability to do so should be considered as the author's inalienable right to connect with the readers. What was more important for Kant was the safeguarding of an author's right to connect with the readers rather than the author's property rights over the means of that connection, i.e. the book. For Kant, the freedom of the pen is the only safeguard of the rights of the people<sup>4</sup>. Kant does not endorse the thesis that ideas can be privately owned. He believed that only physical things can be owned and their purchasers as legitimate owners are free to copy them and even sell their reproductions.

Kant draws a distinction between the book as a physical object and the thoughts it conveys. The book as a physical object becomes a property of whoever buys it. For this reason, Kant believed, that it is not fair to restrain the ways in which its legitimate purchaser may use it without his consent. Therefore, it is undeniable that the property owner of a book may even copy it at his sole will. But, the book also contains the thoughts that are published through it, which in Kant's theory, remain a property of the author of the book regardless of their reproduction. The original thoughts of the author should not be miss-replaced with the physical resources which convey them. The connection between the author and his ideas

---

3. Pozzo, R., (2006), *Immanuel Kant on intellectual property*, v.29, no.2, pp. 11-18, available at <http://www.scielo.br/pdf/trans/v29n2/v29n2a02.pdf> [last check, Apr. 20, 2011].

4. Williams, G. (2009), *Kant's account of reason*, Stanford Encyclopedia of Philosophy, available at <http://plato.stanford.edu/entries/kant-reason/> [last check, Apr. 20, 2011].

From Kant's "*What is Enlightenment?*" (1784) work the author posits that Kant is not primarily concerned with enlightenment as the activity or condition of an individual: rather as something that human beings must work towards together. For this, he says, *nothing is required but... the least harmful... freedom: namely, freedom to make public use of one's reason in all matters* (8:36). This is not the freedom to act politically. Rather, it is what we now call freedom of the pen-in Kant's words, the use of reason *as a scholar* before the entire public of the world of readers (8:37). See also Fauscher, F., (2007), *Kant's social and political philosophy*, Stanford Encyclopedia of Philosophy, available at <http://plato.stanford.edu/entries/kant-social-political/index.html#RepEnlDem> [last check, Apr. 20, 2011].

will continue to exist regardless of them being thought by everyone and/or the property status of their written expressions.

For Kant, the unbreakable connection between an author and his ideas is the result of the fact that ideas are not physical resources. When physical resources are the property of an individual, they cannot be owned and used by everyone else. Yet, with ideas this is not the case. Ideas can be reproduced and thought by everyone without depriving their authors. Kant believed that knowledge is not a physical object exposed to rivalrous use. For this reason it is senseless to submit it to private property and to forbid the reproduction of ideas. On the other hand, it is equally senseless to forbid the reproduction of any physical object if it has been purchased in a legal transaction and the purchaser copies it by his own means. Therefore, if intellectual property is meant to be a right on the physical objects any reservation on copyright is untenable.

Kant believed that a book, through which an author's ideas are published, is not merely a physical object, but also the medium through which an author can transmit his ideas to the public. The medium is provided by the publisher who, thus, speaks to the public in the name of the author, and only if the former has the latter's authorization. The mandate of the author to the publisher, Kant believed, is only a personal relationship that does not imply the acquisition of proprietary rights on the texts. The goal of this personal relationship is conveying a speech to the public. The author speaks to the public and the public has the right to his speech regardless to the publisher, whose rights are justified only to the point that he provides the author the medium to reach the public<sup>5</sup>. Kant justified the reproduction of texts for personal use—he saw no piracy in the reproduction for personal use that was non-commercial, too, by his time. Kant believed that the problem of unauthorized reproduction is that the reproducer acquires the capability to speak to the public without the author's authorization. But if the said reproduction of the text that conveys an author's speech is aimed for personal use (a.k.a. non-commercial use), then the reproducer does not speak to the public in the name of the author, thus the reproduction of the text even without an author's authorization is justified.

There is no specific consideration for the commons in the Kantian theory, at least in the same clear sense that said consideration is made in the Lockean theory. Probably this explains why theories on the wealth of the public domain in continental European Law with the Kantian tradition are quite different in perspective

---

5. Pievatolo, C.M., (2010), *Freedom, Ownership and Copyright: why does Kant reject the concept of intellectual property?*, available at <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1540095](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1540095)> [last check, Apr. 20, 2011].

than theories on the same subject in the Lockean-based legal tradition of the U.S. Contrary to the situation in the U.S., in Europe legal literature only recently developed on the subject of the public domain mostly elaborating upon the perspective that relates to the duration of the author's rights protection<sup>6</sup>. The fact that Europe is lagging compares to the U.S. in the discussion about the public domain is as much impressive as odd. Despite the lacking of a meaningful elaboration upon public domain as a commons in the Kantian theoretical approach to copyright in continental European legal tradition, the origins of the public domain are traced not in the American, but rather in Europe and more specifically in the French inventive philosophical elaborations<sup>7</sup>.

Debates in Europe regarding the duration of copyright protection have reached at an impasse, and it does not seem that there is any room for an agreement among negotiating parties. The debate in Europe as well as internationally and beyond the European legal tradition<sup>8</sup> upon the applicability of Victor Hugo's proposal

---

6. For a critical overview of the U.S. and European legal regimes upon Copyright, see Spinello, R., and Bottis, M., (2009), *A defense of intellectual property rights*, Edward Elgar, pp. 50-114.

7. French Copyright law in effect before the pass of the Berne Convention provisioned the public domain. Said provisioning was the cause for article 14 of the Berne Convention of 1886 that provided as follows: *Under the reserves and conditions to be determined by common agreement, the present Convention shall apply to all works which at the moment of its coming into force have not yet fallen into the public domain in the country of origin*. See more regarding the origins of the public domain at Ochoa, T., (2002), *Origins and meanings of the public domain*, 28 University of Dayton Law Review, pp. 215-266, available at <<http://law.scu.edu/faculty/File/ochoa-tyler-origins-meanings-public-domain.pdf>> [last check, Apr. 20, 2011]; Samuelson, P., (2006), *Challenges in mapping the public domain*, Chapter II in Lucie Guibault and P. Bernt Hugenholtz eds., (2006), *The future of the public domain: identifying the commons in information law*, Kluwer Law International; Dusollier, S., (2010), *Scoping study on copyright and related rights and the public domain*, WIPO CDIP/4/3/REV./STUDY/INF/1, p. 16, available at <[http://www.wipo.int/meetings/en/doc\\_details.jsp?doc\\_id=147012](http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=147012)> [last check, Apr. 20, 2011]; Ginsburg, J., (2006), *Une chose publique? The author's domain and the public domain in early British, French and US copyright law*, Cambridge Law Journal, 2006, Columbia Public Law Research Paper No. 06-120, available at <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=928648](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=928648)> [last check, Apr. 20, 2011].

8. See UNESCO, (1982), *Committee of Non-Governmental experts on the 'Domaine Public Payant'*, Geneva, Switzerland, Apr. 26-29, 1982, XVI Copyright Bulletin, 3, pp. 46-54; United Nations Educational, Scientific and Cultural Organization & WIPO, (1982), *Analysis of the replies to the survey of existing provisions for the application of the system of 'Domaine Public Payant' in national legislation*, Committee of Non-Governmental Experts on the 'Domaine Public Payant', UNESCO/WIPO/DPP/CE/1/2, Mar. 10, 1982, available at <<http://unesdoc.unesco.org/images/0004/000480/048044EB.pdf>> [last check, Apr. 20, 2011]; UNESCO, (1990), XXIV Copyright Bulletin, 4, 1990, pp. 14-28, available at <<http://unesdoc.unesco.org/images/0008/000885/088519eo.pdf>> [last check, Apr. 20, 2011].

for the '*domaine public payant*' (paying the public domain) regarding the use of works that were no longer protected by copyright and have fallen into the public domain<sup>9</sup>, has also reached a dead-end point mainly due to its controversial nature, and mainly because the remuneration fee for public domain works is an impediment to the free use of public domain material<sup>10</sup>; it is a form of compulsory licensing or taxation for works that are supposed to be free of any copyright restrictions<sup>11</sup>. The current perspective in most European Community Members' copyright debates regarding the public domain revolves around copyright's inherent limits that are designed to promote the dissemination of new works or inventions and to ensure the preservation of a vigorous public domain. Said limits are the definition of protected subject matter, the criteria for protection, the fixed duration of the intellectual property protection, and the exhaustion doctrine<sup>12</sup>.

What is Immanuel Kant for the history of copyright in continental Europe and the author's inalienable right approach is John Locke for the history of copyright in the Anglo-Saxon, and especially in the United States legal tradition.

## John Locke

In 1690 John Locke published his "*Two Treatises of Civil Government*" in which he posted that in the beginning "*earth and all inferior creatures*" are common to everybody. But every individual who mixes with what nature has provided with

- 
9. Victor Hugo's '*domaine public payant*' proposal pertains to the possibility of imposing a remuneration right to the author's heirs or assignees for works that lapsed into the public domain or imposing said right to a cultural fund with the aim to collect and distribute subsidies to subsequent authors with a view to help the creation and enlargement of the public domain. Hugo made his proposal in one of his speeches before Congr s Litt raire International that was given in June 25, 1878. See more upon the European public domain perspective at Guibault, L., (2006), *Wrapping information in contract: how does it affect the public domain?*, Chapter V in Lucie Guibault and P. Bernt Hugenholtz eds., (2006), *The future of the public domain: identifying the commons in information law*, Kluwer Law International; d'Ormesson-Kersaint, B., (1983), *La protection des oeuvres du domaine public*, 116 *Revue internationale du droit d'auteur*, pp. 73-151.
  10. See Kallinikou, D., (2008), *Intellectual property and related rights*, 3<sup>rd</sup> ed. Sakkoulas, pp. 234-235 (in Greek).
  11. The idea of providing remuneration from the publication of works in the public domain with the aim to benefit current creators exists nowadays in the legislation of some countries such as Algeria, Kenya, Ruanda, Senegal, Congo, and Paraguay. It was also included in the Copyright law of Italy as *Diritto Demaniale* (Domain Right) until 1996 when said law was amended and said remuneration was abrogated. See more in Dusollier, S., (2010), *ibid*, pp. 40-42.
  12. Guibault, L., (2006), *ibid*, p. 91.

his own labor creates something new and, thus, makes it his property<sup>13</sup>. For John Locke property meant what men have in their persons as well as goods<sup>14</sup>. This conception of property meant that Locke included intangibles such as intellectual assets in his vision of what the concept of property covered since what men have in their persons referred to property associated with men's personality that could be of an intangible nature<sup>15</sup>.

In Chapter V of the Second Treatise, Locke remarked that every man has a property in his own person in which nobody has any right to but himself<sup>16</sup>. Locke expressed a natural law viewpoint for the appropriation of resources based on labor and a man's natural right to enclose within his individual sphere of control the fruits of his labor<sup>17</sup>. For some scholars<sup>18</sup> this remark by Locke may support common ground with the Kantian theory associating copyright to the personality of authors<sup>19</sup>. John Locke's essay "*Labour*"<sup>20</sup>, which was published only a year before the "*Liberty of the Press*" and five years after the Second Treatise, clarified that

---

13. This is the so called Locke's '*mixing argument*'. See more upon it in Spinello, R., and Bottis, M., (2009), *ibid*, pp. 150-155.

14. Locke, J., (1967), *Two treatises of government, second treatise, (1690)*, §§ 25-51 at pp. 302-351, and § 173, p. 401, in Peter Laslett ed., 2<sup>nd</sup> ed., Cambridge University Press; the same, (1988), *An essay concerning the true original, extent, and end of civil government, in two treatises of government*, Chapter V, p. 27, Peter Laslett ed., Cambridge University Press.

15. Zemer, L., (2006), *The making of a new copyright lockean*, 29 Harvard Journal of Law & Public Policy 3, pp. 891-947, p. 907, available at <[http://www.law.harvard.edu/students/orgs/jlpp/Vol29\\_No3\\_Zemer.pdf](http://www.law.harvard.edu/students/orgs/jlpp/Vol29_No3_Zemer.pdf)> [last check, Apr. 20, 2011].

16. Locke, J., (1967), *ibid*, § 27, pp. 305-306, and § 44, p. 316.

17. Spinello, R., and Bottis, M., (2009), *ibid*, p. 171, where the authors recognize that Locke's deontic philosophical views seem to be closer to the European legal perspective which focus on the author's natural rights than the current U.S. legal perspective of utilitarianism in Copyright law.

18. See, for example, Benkler, Y., (2001), *Siren songs and amish children: autonomy, information and the law*, 76 New York University Law Review, p. 59, who points that the basic ideological commitment of U.S. intellectual property law is heavily utilitarian, not Lockean or Hegelian. See, also, Spinello, R., and Bottis, M., (2009), *ibid*, p. 178, who accept that the Lockean model basing limited property rights in the author's right to his or her labor is the most morally persuasive non-utilitarian rationale in intellectual property; and is also a sufficient basis upon which the reconciliation of exclusive intellectual property rights with the common good as is expressed in a robust intellectual commons could happen.

19. Zemer, L., (2006), *ibid*, p. 908, note 80; Rose, M., (1995), *Authors and Owners: The Invention of copyright*, 2<sup>nd</sup> ed., Harvard University Press.

20. Locke, J., (1997), *Labour (1693)*, reprinted in *Locke: political essays*, pp. 326-328, Mark Goldie ed., Cambridge University Press.

when he used the term property he referred to both tangible and intangible<sup>21</sup>. In this essay, Locke addressed issues of manual labor performed by country men and intellectual labor performed by gentlemen and scholars.

In Locke's labor theory-that has an effect on intellectual labor as well-there is a union of two complementary theses. First, the thesis that everyone has a natural property right in the labor of his body and, obviously, his mind, too<sup>22</sup>; and second, the thesis that a property right is limited by specific social norms<sup>23</sup>. The Lockean approach to property-including intellectual property-rights requires that those rights must be properly configured to ensure that others are not harmed by the acquisition of property.

Locke's theory demands that property rights be limited by the concern for the public domain and the common good. The bestowal of property and intellectual property rights should not cause any harm to others through a wasteful depletion of the commons. Locke's labor theory was affected by influential French philosophers and thinkers such as Voltaire and Jean-Jacques Rousseau, as well as many Scottish Enlightenment thinkers and American revolutionaries. Locke's contributions to classical republicanism and liberal theory are reflected in the American Declaration of Independence. Locke's ideas had an impact on the philosophy of the late eighteen and nineteen centuries in Europe, according to which an author was deemed to vest his work in the public sphere, i.e. society, through the mere act of publishing<sup>24</sup>.

In that sense, thinkers such as Augustine Charles Renouard<sup>25</sup>, Isaac René Guy Le Chapelier<sup>26</sup>, and Victor Hugo<sup>27</sup> in France the England considered authors as serv-

---

21. Zemer, L., (2006), *ibid*, pp. 910-911.

22. Spinello, R., and Bottis, M., (2009), *ibid*, p. 152.

23. Zemer, L., (2006), *ibid*, pp. 914-918.

24. See more on the history and origins of Copyright in the U.S. and Europe in Ginsburg, J., (1990), *A tale of two copyrights: literary property in revolutionary France and America*, 64 *Tulane Law Review*, pp. 991-1031, available at <<http://www.compilerpress.ca/CW/Library/Ginsberg%20Tale%20of%20Two%20Copyrights%20TLR%201990.htm>> [last check, Apr. 20, 2011].

25. Renouard, A.Ch., (1839), *Traite des droits d' auters, dans la literature, les sciences at les beaux-arts*, Paris, available through <<http://www.archive.org/details/traitedesdroitsd00reno-goog>> [last check, Apr. 20, 2011].

26. Isaac René Guy Le Chapelier was a French jurist and politician of the French Revolution period, a.k.a. 1789-1799.

27. In his speech of 1878 entitled '*Domain public payant*', Hugo advocated the creation of a property right in favor of authors on their works, coupled with the right of publishers to publish all works after the death of their author under the sole condition that a very low royalty



ants of the public to which they contributed their intellectual work aiming at the growth of knowledge<sup>28</sup>. Also, the utilitarian theorists such as Jeremy Bentham<sup>29</sup> and John Stuart Mill<sup>30</sup> leveraged on Locke's labor theory with the aim to explicitly apply it to informational goods. In that sense, creative works represented for utilitarianism one of the purest forms of an individual's labor and personality. A few years before publishing his seminal work "Two Treatises of Civil Government", John Locke had drafted a memorandum on the 1662 Licensing Act<sup>31</sup> to the Parliament urging it to abolish of the old publishers' privileges and to replace

---

not exceeding 5-10% of the net revenue be paid to the direct heirs of author. See Hugo, V., (2005), *Discours d'ouverture du Congrès littéraire international de 1878* available at <[http://www.inlibroveritas.net/lire/oeuvre1923.html#page\\_1](http://www.inlibroveritas.net/lire/oeuvre1923.html#page_1)> [last check, Apr. 20, 2011].

28. The following often quoted statement of Le Chapelier introduced the idea of a public domain within the copyright system itself: The most sacred, the most legitimate, the most indisputable, and if I may say so, the most personal of all properties is the work which is the fruit of writer's thoughts. But it is a property of a different kind from all the other properties. [Once the author has disclosed the work to the public] the writer has affiliated the public with his property, or rather has fully transmitted his property to the public. However, because it is extremely just that men who cultivate the domain of ideas be able to draw some fruits of their labours, it is necessary that, during their whole lives and some years after their deaths, no one may, without their consent, dispose of the product of their genius. But also, after the appointed period, the public's property begins, and everyone should be able to print and publish the works that have contributed to enlighten the human spirit. See more in Du-sollier, S., (2010), *ibid*, p. 17.
29. Jeremy Bentham (1748–1832) is the father of utilitarianism. He was an English jurist, philosopher, and legal and social reformer. He became a leading theorist in Anglo-American philosophy of law and a political radical whose ideas influenced the development of welfarism. He is best known for his advocacy of utilitarianism.
30. John Stuart Mill (1806–1873), a British philosopher, economist, moral and political theorist, and administrator, was the most influential English-speaking philosopher of the nineteenth century. His views are of continuing significance, and are generally recognized to be among the deepest and certainly the most effective defenses of empiricism and of a liberal political view of society and culture. His views are not entirely original, having their roots in the British empiricism of John Locke, George Berkeley and David Hume, and in the utilitarianism of Jeremy Bentham.
31. The 1662 Act was titled *An act for preventing the frequent abuses in printing seditious treasonable and unlicensed Books and Pamphlets and for Regulating of Printing and Printing Presses*, and its main goal was to control the press.

them with what seemed a more author-centric copyright approach<sup>32</sup>. Thus, John Locke could justifiably be considered Copyright's über-father<sup>33</sup>.

John Locke's opposition to the 1662 Licensing Act was also explicit in the 1694 letter titled "*Liberty of the Press*"<sup>34</sup> in which he opposed the renewal of the Licensing Act of 1662<sup>35</sup>. The Act was a punitive instrument for controlling printing presses. It restricted the number of printing presses and revived the practice in which all publications had to be approved by the Licenser. According to the 1662 Act, the entrance of a book or copy in the Register, i.e. the Government, was deemed to vest a perpetual copyright in the stationer, i.e. the publisher, who entered it. John Locke opposed to the control of printing presses by the Government through the stationers guild, and elaborated upon the reasons for abolishing Government's monopoly over printing presses; he argued in support of readers' free access to literature and scholarship encouraging the unobstructed study and dissemination of knowledge<sup>36</sup>.

Locke contended that the monopoly and excessive powers of the Government-controlled Stationers' Company<sup>37</sup> over the printing presses adversely affected the dissemination of knowledge and the availability of classic authorial works affect-

---

32. Hughes J., (2006), *Locke's 1964 Memorandum (and more incomplete Copyright historiographies)*, introductory essay, an accompanying piece to Justin Hughes' *Copyright and incomplete historiographies: Of piracy, proprietization, and Thomas Jefferson*, 79 Southern California Law Review, p. 993, Cardozo Legal Studies Research Paper No. 166, available at <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=934869](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=934869)> [last check, Apr. 20, 2011].

33. Mayer-Schönberger, V., (2005), *In search of the story: narratives of the intellectual property*, 10 Virginia Journal of Law & Technology, 11, available at <[http://www.vjolt.net/vol10/issue4/v10i4\\_a11-Mayer-Schonberger.pdf](http://www.vjolt.net/vol10/issue4/v10i4_a11-Mayer-Schonberger.pdf)> [last check, Apr. 20, 2011].

34. Locke, J., (1997), *Liberty of the press (1695)*, reprinted in *Locke: political essays*, Mark Goldie ed., Cambridge University Press.

35. Astbury, R., (1978), *The renewal of the licensing Act in 1693 and its lapse in 1695*, 33 Library (5<sup>th</sup> Ser.), pp. 296-297.

36. Zemer, L. (2006), *ibid*, p. 899.

37. In England the printers, known as stationers, formed a collective organization, the Stationers' Company. In the 16th century the Stationers' Company was given the power to require all lawfully printed books to be entered into its Register. Only members of the Stationers' Company could enter books into the Register. This meant that the Stationers' Company achieved a dominant position over publishing in 17<sup>th</sup> century England. But the monopoly, granted to the Stationers' Company through the Licensing Act 1662, came to an end when parliament decided to not renew the Act after it lapsed in May 1695. See more for the Worshipful Company of Stationers and Newspaper Makers, i.e. the Stationers' Company, available at Wikipedia at <[http://en.wikipedia.org/wiki/Stationers'\\_Company](http://en.wikipedia.org/wiki/Stationers'_Company)> [last check, Apr. 20, 2011]; also, at Spinello, R., and Bottis, M., (2009), *ibid*, pp. 18-19.

ing negatively scholars, authors and the public at large. The Crown had vested the Stationer's Company with the power to decide upon the printing of a book on condition of registration with it. All lawfully printed books had to be recorded in the Company's register. The right to make an entry to the Register was confined by the Crown to the register of the Company's members, who were furnished with perpetual copyright on the books that were published after proper registration<sup>38</sup>. Authors of said books were not, and could not become, members of the Stationers' Company, thus no copyright was possible for them.

Additionally, Locke supported limiting the duration of an author's right as vital so that knowledge could become available to the public without any proprietary right limitations. In that sense, Locke claimed that the 1662 Act violated the three basic rights of trade, liberty and property meaning that the perpetual rights vested to the Stationers' Company denied an author his property rights and violated his liberty to exchange and trade his own property<sup>39</sup>. Locke remarked that nobody should have any peculiar right in any book which had been in print for fifty years, and supported a term of years for copyright followed by a lapse into the public domain<sup>40</sup>. This term, Locke supported, should be either fifty years after the first publication of the book, or fifty or seventy years after the death of author in case the author's work had not been published during his lifetime.

John Locke's approach on copyright was an extension of his labor theory of property. It had a deep impact and influenced utilitarianism<sup>41</sup>, and it was mainly this utilitarian approach<sup>42</sup> that affected world's first copyright law, the Statute of

---

38. The Stationers' Company was empowered by the Crown with police-like powers of search and seizure of books which were not registered. The Crown was using the Stationer's Company as ready-made agents of censorship. See more at Spinello, R., and Bottis, M., (2009), *ibid*, p. 15-19.

39. Zemer, L., (2006), *ibid*, p. 903; Locke, J., (1997), *ibid*, p. 333.

40. Zemer, L., (2006), *ibid*, p. 905 ; Locke, J., (1997), *ibid*, p. 337.

41. Utilitarianism (also: utilism) is the idea that the moral worth of an action is determined solely by its usefulness in maximizing utility and minimizing negative utility (utility can be defined as pleasure, preference satisfaction, knowledge or other things) as summed among all sentient beings. It is thus a form of consequentialism, meaning that the moral worth of an action is determined by its outcome. The most influential contributors to this theory are considered to be Jeremy Bentham and John Stuart Mill. See more upon Utilitarianism at Wikipedia, available at <<http://en.wikipedia.org/wiki/Utilitarianism#History>> [last check, Apr. 20, 2011].

42. The utilitarian approach focuses on the general good which is described in terms of 'utility' for the general public. Utility becomes the foundation of morality and the ultimate criterion of right or wrong; it is the sum of the net benefits caused by an action.

Anne in 1709<sup>43</sup>. The utilitarian approach to copyright<sup>44</sup> was passed to the American Constitution's provisions<sup>45</sup> for the protection of copyright since the drafting process of the Constitution by the time of Thomas Jefferson<sup>46</sup>. The U.S. Federal Copyright Act of 1790<sup>47</sup>-the first U.S. Copyright Law<sup>48</sup>-was one of the first laws passed by the U.S. Congress, which Act gave authors an exclusive right to their creations for the duration of fourteen years from the date of compliance with

---

43. *The Statue of Anne*, available at <[http://en.wikipedia.org/wiki/Statute\\_of\\_Anne](http://en.wikipedia.org/wiki/Statute_of_Anne)> [last check, Apr. 20, 2011]; it was titled *An Act for the Encouragement of Learning, by Vesting the Copies of printed Books in the Authors, or Purchasers, of such Copies during the Times therein mentioned*. See more upon the Statute of Anne at Spinello, R., and Bottis, M., (2009), *ibid*, pp. 19-26.

44. The utilitarian approach to copyright posits that copyright's essence is to enhance over social welfare by providing an incentive for new innovation where social welfare is understood as the maximization of aggregate wealth that society gets from its scarce resources. Intellectual property rights are necessary in order to maximize social welfare by providing authors and other creators with a reward that is secured through Copyright's provisions for strongly protected intellectual property rights. Without these strong rights, authors and other creators would have no incentive to create, thus society would suffer from loss of creations and inventions. Without strong Copyright laws, people would be more inclined to use works regardless of authors' will and against authors' interests to recoup their investments spent in the creative process. See more about classic utilitarianism in Spinello, R., and Bottis, M., (2009), *ibid*, pp. 167-171.

45. The U.S. Constitution in Article I, Section 8, Clause 8 confers upon the Congress the power "To promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries" by awarding exclusive property rights.

46. Thomas Jefferson served as a delegate to the Second Continental Congress beginning in June 1775, soon after the outbreak of the American Revolutionary War. When Congress began considering a resolution of independence in June 1776, Jefferson was appointed to a five-man committee to prepare a declaration to accompany the resolution. The committee selected Jefferson to write the first draft probably because of his reputation as a writer. Jefferson completed a draft in consultation with other committee members, drawing on his own proposed draft of the Virginia Constitution, George Mason's draft of the Virginia Declaration of Rights, and other sources. See more upon Thomas Jefferson, available at <[http://en.wikipedia.org/wiki/Thomas\\_Jefferson#Drafting\\_a\\_declaration](http://en.wikipedia.org/wiki/Thomas_Jefferson#Drafting_a_declaration)> [last check, Apr. 20, 2011]. See, also, <<http://www.archives.gov/exhibits/charters/>> [last check, Apr. 20, 2011] for the making of the Charters, the Declaration of Independence, The Constitution of the United States, the Bill of Rights and the impact of the Charters.

47. See more on *U.S. Copyright Act of 1790* available at Wikipedia at <[http://en.wikipedia.org/wiki/Copyright\\_Act\\_of\\_1790](http://en.wikipedia.org/wiki/Copyright_Act_of_1790)> [last check, Apr. 20, 2011].

48. For a brief introduction and history of U.S. Copyright Law, see United States Copyright Office available at <<http://www.copyright.gov/circs/circ1a.html>> [last check, Apr. 20, 2011].

certain notice, deposit, and recordation procedures. The 1790 Act also provided that, if the author survived the initial term, he or his “executors, administrators or assigns” could renew the copyright for a renewal term of another fourteen years.

## The no-harm principle

In John Locke’s labor theory for the appropriation of intellectual property balance between copyright of the labourer and the protection of the common good is framed by the no-harm principle<sup>49</sup>. Locke believed that under certain conditions an individual’s acquisition of property should not violate anyone’s right to property in the commons<sup>50</sup>, i.e. intellectual labor creates a property entitlement in so far as it does not limit a person’s rights to intellectual property in the common<sup>51</sup>. For Locke, labor as well as intellectual labor is the basis for a property right instead of a mere use right because without that right to control one’s labor and exclude others from the product of it self-governance becomes impossible.

However, Locke through the no-harm principle suggested that a person’s natural property right based on his labor is protected only when it is balanced against and regulated by certain social norms so that it did not conflict with the com-

---

49. Spinello, R., and Bottis, M., (2009), *ibid*, p. 9.

50. The terms “public property” or “common property” or “publici juris” were first used in 19<sup>th</sup>-century by American courts in order to refer to non-copyrightable and non-patentable subject matter. The term “publici juris” is first met in the 1774 *Donaldson v. Beckett* case brought in front of English court as a reference to statutory term once copyright protection has ended. In the late 19<sup>th</sup> century the term “public domain” began to appear occasionally in patent decisions. These three terms were initially used by 19<sup>th</sup>-century American courts in order to describe both materials for which patent and copyright protection had expired as well as material definitionally ineligible for protection. Gradually, however, these terms fell into disuse in intellectual property law, while the only term used to describe the boundary between the proprietary and the public is the term “*public domain*.” See more for the evolution of these terms in Lee E., (2003), *The Public’s Domain: The Evolution of Legal Restraints on the Government’s Power to Control Public Access Through Secrecy or Intellectual Property*, 55 *Hastings Law Journal*, pp. 91-209, available at [http://www.estig.ipbeja.pt/~ac\\_direito/lee.pdf](http://www.estig.ipbeja.pt/~ac_direito/lee.pdf) [last check, Apr. 20, 2011]; Ochoa, T., (2002), *ibid*; Cohen, J., (2006), *Copyright, Commodification, and Culture: Locating the Public Domain*, Chapter IV in Guibault, L., & Hugenholtz, P.B., eds., pp. 121-166, Kluwer Law International, 2006, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=663652](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=663652) [last check, Apr. 20, 2011].

51. In the famous English case *Donaldson v. Beckett* (1774), Lord Camden famously equated science and learning to *things common to all mankind, that ought to be as free and general as air or water*. See more about the case in <http://www.copyrighthistory.com/donaldson.html> [last check, Apr. 20, 2011].

mon good<sup>52</sup>. The labourer himself has the principal claim on the output of his labor which is per se sufficient justification for the appropriation of objects and resources and their integration into the labourer's private sphere of influence. However, the same labor is also sufficient justification for the enlargement of social wealth in the sense that labor adds new value and creates social wealth for labor puts the difference of value on everything<sup>53</sup>. If the appropriation of labor's output ends up with scarcity of wealth to the detriment of social benefit, then appropriation per se is the cause of an imbalance in society and labor transforms from a power to create wealth into a cause for the depletion of wealth. Similarly, if an author's appropriation of labor's output cannot end up with the creation of wealth that he has a natural right upon, then labor is insufficient as a foundation for progress.

The centrepiece of the Lockean theory is the labor as a means to create wealth. Labor is justified as the foundation upon which wealth and progress can be based on condition that labor meets the interests of both the creator and society's. The safety valve in the Lockean theory upon the justification of labor as a means to create wealth and cause progress is the no-harm principle that balances individual and social interests<sup>54</sup>.

Locke's no-harm principle evangelizing balance between proprietary rights and public property became the central theme of the seminal 1896 Supreme Court of the U.S. decision in the case *Singer Manufacturing Co. v. June Manufacturing Co.*<sup>55</sup>, which is a landmark verdict regarding copyright theory and related legal terminology regarding the public domain. The case concerned the eligibility of the name 'Singer' for protection following expiration of the Singer Manufacturing Company's patents on its sewing machines. The Supreme Court quoted Justice Miller's discussion of 'public property' as well as British and French provisions regarding the subject matter of expired patents, and linked all these information to the idea of the 'public domain' in which such property-i.e. the name

---

52. Zemer, L., (2006), *ibid*, p. 918.

53. Attas, D., (2009), *Lockean Justifications of Intellectual Property*, in Alex Gosseries, Alain Marciano and Alain Strowel (eds.) *Intellectual Property and Theories of Justice*, Palgrave Macmillan, p. 29.

54. Spinello, R., and Bottis, M., (2009), *ibid*, p. 206, who recognize in Locke's views the proper intellectual and normative background and intellectual property's foundation in the sense of an equilibrium between an author's interests and the interests of the general public for authorial works of intellect; they supplement said normative background and copyright's foundation with the Hegelian theory's sensitivity to personhood interests.

55. *Singer Manufacturing Co. v. June Manufacturing Co.*, 163 U.S. 169, 203 (1896), available at <<http://supreme.justia.com/us/163/169/case.html>> [last check, Apr. 20, 2011].

'Singer'-resided. Said U.S. Supreme Court case concluded that 'the world 'Singer', as we have seen, had become public property, and ...it could not be taken by the Singer Company out of the public domain by the mere fact of using that name as one of the constituent elements of Singer Company's trade-mark.' After the U.S. Supreme Court verdict in the case *Singer Manufacturing Co. v. June Manufacturing Co.*, courts gradually began to adopt the terminology 'public domain'<sup>56</sup>. At an international level, the term 'public domain' was first used in the legal text of the 1886 Berne Convention article 14 which provided that "Under the reserves and conditions to be determined by common agreement, the present Convention shall apply to all works which at the moment of its coming into force have not yet fallen into the public domain in the country of origin"<sup>57</sup>.

### The no-spoliatio proviso

The social norms in Locke's no-harm principle are composed by two immediate conditions; the first condition is known as "*the no-spoliatio proviso*", which posits that the laborer may appropriate only the amount that he can use. This is the meaning in Locke's words "*nothing was made by God for Man to spoil or destroy*"<sup>58</sup>. Locke's no-spoliatio proviso is an expression of his awareness that in situations of perpetual rights in works of authorship spoilage of social value is inevitable<sup>59</sup>. For Locke, any system of authors' rights must incorporate the no-spoliatio condition as part of its moral applicability. Locke's ideal of a system that caters for

56. Cohen, J., (2006), *ibid*, p. 126, according to who the legislative impetus for widespread adoption of the 'public domain' term in the U.S. Copyright Law was the enactment of the 1909 Copyright Act in Section 7 expressly excluded copyright protection for 'works in the public domain'. See the amended text of Section 7 of the 1909 Copyright Act at <[http://www.megalaw.com/top/copyright/1909/1909\\_7.php](http://www.megalaw.com/top/copyright/1909/1909_7.php)> [last check, Apr. 20, 2011]. See, also, Ochoa, T., (2002), *ibid*; Rose, M., (2003), *Nine-tenths of the law: the english copyright debates and the rhetoric of the public domain*, 66 *Law & Contemporary Problems*, pp. 75-87, available at [http://www.law.duke.edu/shell/cite.pl?66+Law++Contemp.+Probs.+75+\(WinterSpring+2003\)](http://www.law.duke.edu/shell/cite.pl?66+Law++Contemp.+Probs.+75+(WinterSpring+2003)) [last check, Apr. 20, 2011].

57. See also article 18§1 of the Berne Convention that is available at <[http://www.wipo.int/treaties/en/ip/berne/trtdocs\\_wo001.html](http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html)> [last check, Apr. 20, 2011] as it has been amended and applies today, which posits that *This Convention shall apply to all works which, at the moment of its coming into force, have not yet fallen into the public domain in the country of origin through the expiry of the term of protection.*

58. Zemer, L., (2006), *ibid*, p. 919; Locke, J., (1967), *ibid*, §31, p. 308.

59. Damstedt, B.G., (2003), *Limiting Locke: a natural justification for the fair use doctrine*, 112 *Yale Law Journal*, pp. 1179-1221, available at <<http://www.yalelawjournal.org/the-yale-law-journal/content-pages/limiting-locke-a-natural-law-justification-for-the-fair-use-doctrine/>> [last check, Apr. 20, 2011].

authorial rights respects the requirement of public access to authorial works for educational and learning purposes, and considers perverse any copyright system that prohibits proper access and use of works by the public because of authorial rights<sup>60</sup>. For John Locke, the ideal authorial rights system must ensure that the author-laborer's rights are protected in as much as he is made by the system to leave enough and as good in the common wherefrom he draws resources with the aim to create<sup>61</sup>.

Locke rejected the idea that authors create their works *ex nihilo*. On the contrary, he believed that authors create their works based on pre-existing mental and intellectual raw materials in the commons, i.e. in the public domain. Authors do not create in the vacuum, but rather they create by mixing their mental labor with pre-existing ideas and collectively owned objects<sup>62</sup>. This idea for creativity is still respected in legal theory which understands common resources not simply as the distant backdrop for productive activity that is largely private, but as the infrastructure that supports private productive activity and enables its success<sup>63</sup>.

---

60. Zemer, L., (2006), *ibid*, pp. 922-925.

61. Zemer, L., (2006), *ibid*, p. 933.

62. Zemer, L., (2006), *ibid*, p. 936, and p. 945, according to who John Locke writes in Book IV of his work *An essay concerning human understanding* (1690), Peter H. Nidditch ed., Oxford University Press 1975, ch.iv, § 3, p. 563: *Our Knowledge therefore is real, only so far as there is a conformity between our ideas and the reality of things*; the meaning in Locke's words is that knowledge is never innate, but rather is socially constructed. Locke believed that knowledge is the outcome of experience, social and cultural exposure and communication, and thus the public plays an important role in the process of an author's creativity in the sense that copyrighted works are depended on an author's capacity to act as a sociable creature.

63. Cohen, J., (2006), *ibid*, p. 139. See, also, Rose, M., (1986), *The comedy of the commons: commerce, custom and inherently public property*, 53 University of Chicago Law Review, pp. 711-781; the same, (2003), *Romans, roads, and romantic creators: traditions of public property in the information age*, 66 Law and Contemporary Problems, pp. 89-110, available at <http://www.law.duke.edu/pd/papers/rose.pdf> [last check, Apr. 20, 2011]; Hess, C., and Ostrom, E., (2003), *Artifacts, facilities, and content: information as a common-pool resource*, 66 Law and Contemporary Problems, pp. 111-145, available at <http://www.law.duke.edu/pd/papers/ostromhes.pdf> [last check, Apr. 20, 2011]; Lessig, L., (2001), *The future of ideas: the fate of the commons in a connected world*, Vintage Books, available at <http://www.the-future-of-ideas.com> [last check, Apr. 20, 2011]; Benkler, Y., (2003), *Through the looking glass: Alice and the constitutional foundations of the public domain*, 66 Law and Contemporary Problems, pp. 173-224, available at [<http://www.law.duke.edu/shell/cite.pl?66+Law+&+Contemp.+Probs.+173+\(WinterSpring+2003\)>](http://www.law.duke.edu/shell/cite.pl?66+Law+&+Contemp.+Probs.+173+(WinterSpring+2003)) [last check, Apr. 20, 2011]; Boyle, J., (2003), *ibid*, pp. 33-74, available at [<http://www.law.duke.edu/pd/papers/boyle.pdf>](http://www.law.duke.edu/pd/papers/boyle.pdf) [last check, Apr. 20, 2011]; Litman, J., (1990), *The Public Domain*, 39 Emory Law Journal, pp. 965-1023.



Thus, Locke believed that public interest in authorial works and proprietary rights in them are interrelated and must be kept in balance, otherwise an authorial system is doomed to fail. For Locke, an authorial system, a copyright law system which grants authors unconditional monopoly-type rights for their works and which withholds optimal public access to copyrighted materials, will eventually have adverse effects on the public interests and is bound to fail for that cause. Locke thought of the public good and was a proponent of the idea that property must be limited in order to maintain a stable social order. In that sense, authorial property should be carefully balanced against certain social norms. Locke was not a defender of a robust system of natural property rights for authors unencroachable by norms of equality and public good. Both in his *Second Treatise of the "Two Treatises of Civil Government"* and in his *"Liberty of the Press"* Locke expressed his commitment to the public interest regarding authorial rights, contended that in consideration of public interest there is no reason in nature to preclude a freer system of use of authors' works and concluded that an author's natural right to his works is a dynamic rather than static guarantee changing to meet the needs of different situations<sup>64</sup>.

### The enough and as good proviso

The second condition in Locke's no-harm principle is known as "the enough and as good proviso" under which a man has a right to appropriate from the common as long as there is enough and as good left in the commons for others<sup>65</sup>. In the *"Liberty of the Press,"* Locke justified the imposition of an involuntary harm on authors' rights for matters of public interest and advocated a weaker version of a natural right for authors that is limited in time and is available for purposes of education and learning<sup>66</sup>. The "enough and as good" proviso ensures that a grant of property does no harm to other persons' equal abilities to create or to draw upon the pre-existing cultural matrix and scientific heritage that exists in the commons and where from the author draws and appropriates resources; the enough and as good proviso restricts the ownership of intellectual creations and widens the doorway to new creators<sup>67</sup>.

---

64. Zemer, L. (2006), *ibid*, p. 934-935.

65. Zemer, L., (2006), *ibid*, p. 919; Locke, J., (1967), *ibid*, §27, pp. 305-306.

66. Zemer, L. (2006), *ibid*, p. 921; Shiffrin S.V., (2001), *Lockean arguments for private intellectual property*, in Munzer (ed.), *New Essays in the legal and political theory of property*, Cambridge University Press.

67. Zemer, L., (2006), *ibid*, p. 926.

Locke was fully aware of the importance of preserving a vibrant public domain to promote the formation of ideas, works and the evolution of authors. For him, the authorial rights cannot be held captive in traditional concepts of property and ownership<sup>68</sup>. Locke's theory on labor's justification represents a plausible conception of intellectual property rights and an intelligible ground for appropriation of resources in the commons so long as said appropriation occurs within the bounds of fairness and ethical uprightness in consideration of the interests from both the laborer and society<sup>69</sup>. The Lockean-based entitlement for intellectual property rights is an optimal starting point for policy-making provided that social welfare considerations are not ignored or under-ruled when copyright legislation is crafted and appropriate limits are imposed in respect of an author's rights<sup>70</sup>.

To that point, Locke's interest and views for the public domain considering it as a commons in which cultural and scientific heritage resides and upon which the general public, including authors, have all right to draw materials from but no right to appropriate them in a way that restricts others from accessing materials in the commons, have been revived in contemporary copyright literature and copyright activism that target the imbalances of the stringent copyright system as it has evolved. In his seminal 1981 article titled "*Recognizing the Public Domain*"<sup>71</sup>, David Lange argued that the public domain should be considered as a public right rather than simply the negative or obverse of intellectual property<sup>72</sup>. Jessica Litman has, also, sought to explain the public domain's purpose and to form a coherent theory about it<sup>73</sup>. Among the many reputable supporters for public domain's necessary existence, the need for its reinforcement and/or acknowledgement by proper legal framework, and its use as an opportunity to reconsider copyright in the era of information networks and Internet networking applications used for accessing and using

---

68. Zemer, L., (2006), *ibid*, pp. 946-947.

69. Gordon, W., (1993), *A property right in self-expression: equality and individualism in the natural law of intellectual property*, 102 *Yale Law Journal*, pp. 1533-1609; Dusollier, S., (2010), *ibid*, p. 20.

70. Spinello, R., and Bottis, M., (2009), *ibid*, p. 206.

71. Lange, D., (1981), *Recognizing the public domain*, 44 *Law and Contemporary Problems*, p. 147, available at <[http://www.law.duke.edu/pd/papers/lange\\_background.pdf](http://www.law.duke.edu/pd/papers/lange_background.pdf)> [last check, Apr. 20, 2011].

72. Lange, D., (2003), *Reimagining the Public Domain*, 66 *Law and Contemporary Problems*, pp. 463-483, available at <[http://www.law.duke.edu/shell/cite.pl?66+Law+&+Contemp.+Probs.+463+\(WinterSpring+2003\)](http://www.law.duke.edu/shell/cite.pl?66+Law+&+Contemp.+Probs.+463+(WinterSpring+2003))> [last check, Apr. 20, 2011].

73. Litman, J., (1990), *ibid*.

culture, i.e. knowledge, art and science, are Yochai Benkler<sup>74</sup>, Lawrence Lessig<sup>75</sup>, James Boyle<sup>76</sup>, Pamela Samuelson<sup>77</sup>, Jessica Litman<sup>78</sup>, Jerome Reichman<sup>79</sup>, Mark

- 
74. Benkler, Y., (2003), *ibid*; the same, (2006), *ibid*; the same and Nissenbaum, H., (2006), *Commons-based peer production and virtue*, 14 *The Journal of Political Philosophy*, 4, pp. 394-419, available at <[http://www.nyu.edu/projects/nissenbaum/papers/jopp\\_235.pdf](http://www.nyu.edu/projects/nissenbaum/papers/jopp_235.pdf)> [last check, Apr. 20, 2011]; the same, (1999), *ibid*; the same, (2001), *Siren songs and amish children: Autonomy, information and the law*, 76 *New York University Law Review*, pp. 23-113, available at <<http://www.benkler.org/SirenSongs.pdf>> [last check, Apr. 20, 2011]; the same, (2003), *Freedom in the Commons: towards a political economy of information*, 52 *Duke Law Journal*, pp. 1245-1276, available at <<http://www.law.duke.edu/shell/cite.pl?52+Duke+L.+J.+1245>> [last check, Apr. 20, 2011]; the same, (2000), *ibid*; the same, (2003), *The political economy of commons*, *European Journal for the Informatics Professional*, Upgrade Vol. IV, no.3, June 2003, available at <<http://www.benkler.org/Upgrade-Novatica%20Commons.pdf>> [last check, Apr. 20, 2011]; the same, (2001), *Property, commons, and the first amendment: towards a core common infrastructure*, *Brennan Center for Justice at New York University*, available at <<http://www.benkler.org/WhitePaper.pdf>> [last check, Apr. 20, 2011].
  75. Lessig, L., (2001), *ibid*; the same, (2006), *Re-crafting the public domain*, 18 *Yale Journal of Law & Humanities*, p. 56; the same, (2001), *Architecting Innovation*, *The First Annual Meredith and Kip Frey Lecture in Intellectual Property*, *Duke University*, Mar.23, 2001, video available at <http://www.youtube.com/watch?v=XKLOQy2vRA4>> [last check, Apr. 20, 2011].
  76. Boyle, J., (2003), *ibid*; the same, (2008), *ibid*; the same, (2006), *Tales from the public domain: bound by law?*, *Duke University Center for the Study of the Public Domain*, available at <<http://www.law.duke.edu/cspd/comics>> [last check, Apr. 20, 2011]; the same, (2007), *Cultural environmentalism and beyond*, 70 *Law & Contemporary Problems*, pp. 5-21, available at <[http://www.law.duke.edu/shell/cite.pl?70+Law+&+Contemp.+Probs.+5+\(spring+2007\)](http://www.law.duke.edu/shell/cite.pl?70+Law+&+Contemp.+Probs.+5+(spring+2007))> [last check, Apr. 20, 2011]; the same, (2003), *Forward: the opposite of property?*, 66 *Law & Contemporary Problems*, pp. 1-32, available through <<http://james-boyle.com>> [last check, Apr. 20, 2011].
  77. Samuelson, P., (2003), *Mapping the Digital Public Domain: Threats and Opportunities*, 66 *Law & Contemporary Problems*, pp. 147-171, available at <[http://www.law.duke.edu/shell/cite.pl?66+Law+&+Contemp.+Probs.+147+\(WinterSpring+2003\)](http://www.law.duke.edu/shell/cite.pl?66+Law+&+Contemp.+Probs.+147+(WinterSpring+2003))> [last check, Apr. 20, 2011]; the same, (2001), *Digital Information, Digital Networks, and the Public Domain*, available at <http://www.law.duke.edu/pd/papers/samuelson.pdf> [last check, Apr. 20, 2011].
  78. Litman, J., (1990), *ibid*.
  79. Reichman, J., and Uhler, P.F., (2003), *A contractually reconstructed research commons for scientific data in a highly protectionist intellectual property environment*, 66 *Law & Contemporary Problems*, pp. 315-462, available at [http://www.law.duke.edu/shell/cite.pl?66+Law+&+Contemp.+Probs.+315+\(WinterSpring+2003\)](http://www.law.duke.edu/shell/cite.pl?66+Law+&+Contemp.+Probs.+315+(WinterSpring+2003)) [last check, Apr. 20, 2011].

Rose<sup>80</sup>, Mark Lemley<sup>81</sup>, Julie Cohen<sup>82</sup>, Jonathan Zittrain<sup>83</sup>, Charles Nesson<sup>84</sup>, Diane Zimmerman<sup>85</sup>, Brad Sherman<sup>86</sup>, Michael Birnhack<sup>87</sup>, Charlotte Hess and Elinor Ostrom<sup>88</sup>, Severine Dussolier<sup>89</sup>, Lucy Guibault<sup>90</sup>, Jane Ginsburg<sup>91</sup>, Bernt Huguen-

---

80. Rose, M., (2003), *ibid*.

81. Lemley, M.A., (2005), *ibid*; the same, (2004), *ibid*.

82. Cohen, J., (1998), *ibid*; the same, (1998), *Copyright and the jurisprudence of self-help*, 13 Berkeley Technology and Law Journal, pp. 1089-1143, available at <<http://www.law.berkeley.edu/journals/btlj/articles/vol13/Cohen/html/text.html>> [last check, Apr. 20, 2011]; the same, (2000), *Copyright and the perfect curve*, 53 Vanderbilt Law Review, pp. 1799- 1823, available at <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=240590](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=240590)> [last check, Apr. 20, 2011].

83. Zittrain, J., (2002), *Responses by the research and education communities in preserving the public domain and promoting open access: new legal approaches in the private sector*, National Academy of Sciences, Symposium on the Role of Scientific and Technical Data and Information in the Public Domain, September 6, 2002.

84. Nesson, C., Lessig, L., and Zittrain, J., (1999), *Open code – Open content – Open law, building a digital commons*, Harvard Law School, available at <<http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/opencode.session.pdf>> [last check, Apr. 20, 2011].

85. Zimmermann, D.L., (2004), *Is there a right to have something to say? One view of the public domain*, 73 Fordham Law Review, p. 297.

86. Sherman, B. and Wiseman, L., (2006), *Towards an indigenous public domain?*, Chapter XI in Lucie Guibault and P. Bernt Hugenholtz (eds.) *The future of the public domain – identifying the commons in information law* Kluwer Law International.

87. Birnhack, M., (2006), *More or better? shaping the public domain*, Chapter IV in Lucie Guibault and P. Bernt Hugenholtz (eds.) *The future of the public domain – identifying the commons in information law*, Kluwer Law International.

88. Elinor Ostrom is the 2009 Nobel Laureate in Economy. Hess, C., and Ostrom, E., (2006), *Understanding knowledge as a commons-from theory to practice*, MIT Press; Ostrom, E., (1990), *Governing the commons: the evolution of institutions for collective action*, Cambridge University Press.

89. Dussollier, S., (2009), *The public domain in intellectual property: beyond the metaphor of a domain*, in *Intellectual property and public domain*, pp. 31-69; the same, (2008), *Le domaine public, garant de l'intérêt public en propriété intellectuelle?*, in *L'intérêt général et l'accès à l'information en propriété intellectuelle*, pp. 117-147, available at <http://www.crid.be/pdf/public/5887.pdf> [last check, Apr. 20, 2011]; the same and Benabu, V.L., (2007), *Draw me a public domain*, in *copyright law*, collection research handbooks in intellectual property, pp. 161-184, available at <<http://www.crid.be/pdf/public/5662.pdf>> [last check, Apr. 20, 2011].

90. Guibault, L., (2006), *ibid*.

91. Ginsburg, J., (2006), *ibid*.

holtz<sup>92</sup>, Rosmary Coombe<sup>93</sup>, and William V. Caenegem<sup>94</sup> of whom almost all elaborate upon current copyright's damaging and intrusive application in the commons causing the suffocation of and questioning the survivability of the public domain in a similar way to the description of the so called "tragedy of the commons"<sup>95</sup>. The central idea in the "tragedy of the commons" is that public ownership of a piece of property is inefficient, because non-owners who use the property have no incentive to take care of it and will therefore overuse it<sup>96</sup>.

Almost all contemporary legal theorists and public domain advocates have eloquently expressed the importance of the public domain and its social value to the ongoing creative process and to deliberative democracy. Critics of the current intellectual property regime point to the damage done to the intellectual commons by the privatization and excessive appropriation of resources available in the commons under the provisions of copyright law that cater excessively for authorial "individualism" and "information capitalism" regardless of any public interest in the access to and use of copyrighted works. They contend that the narrow conception of an exclusive individual property right that is over-protected by

---

92. Guibault, L., and Hugenholtz, B., (2006), *The future of the public domain – identifying the commons in information law*, Kluwer Law International; Hugenholtz, B., (2000), *Copyright contract and code: what will remain of the public domain?*, 26 Brooklyn Journal of International Law, pp. 77-90.

93. Coombe, R., (2003), *Fear, hope, and longing for the future of authorship and a revitalized public domain in global regimes of intellectual property*, 52 DePaul Law Review, pp. 1171-1186, available at [http://www.yorku.ca/rcoombe/publications/Fear\\_Hope\\_and\\_Longing.pdf](http://www.yorku.ca/rcoombe/publications/Fear_Hope_and_Longing.pdf) [last check, Apr. 20, 2011].

94. Van Caenegem, W., (2002), *The public domain: scientia nullius*, 24 European Intellectual Property Review, 6, pp. 324-330.

95. The "tragedy of the commons" is a dilemma arising from the situation in which multiple individuals, acting independently and rationally consulting their own self-interest, will ultimately deplete a shared limited resource even when it is clear that it is not in anyone's long-term interest for this to happen. See more about '*The tragedy of the Commons*' in Wikipedia at <[http://en.wikipedia.org/wiki/Tragedy\\_of\\_the\\_commons](http://en.wikipedia.org/wiki/Tragedy_of_the_commons)> [last check, Apr. 20, 2011].

96. Hardin, G., (1968), *The tragedy of the commons*, 162 Science, pp. 1243-1248, available at <<http://www.sciencemag.org/content/162/3859/1243.full.pdf>> [last check, Apr. 20, 2011]. In 1968, Garrett Hardin spoke about the "*tragedy of the commons*" through the example of fish stocks. When a fisherman catches fish of reproductive age, he reduces future fish stocks. The fisherman's action penalizes all fishermen, including himself; but, unlike other fishermen, he offsets the damage to himself with a benefit that he alone appropriates, i.e. a higher catch, so his net situation improves. Every fisherman is tempted to adopt this free riding behaviour, which leads to the depletion of the natural resource and a tragedy of the commons.

regulation which in parallel under-protects the general public's interest in copyrighted works provides an insufficient framework for formulating sound public policy that promotes the social good through regulation that caters for the protection of intellectual property that is deemed to balance private interests and boost creativity in the market for the sake of society<sup>97</sup>.

Instead, what seems to be necessary nowadays is a prudent level of intellectual property protection that is measured and proportionate to an author's need to appropriate a fair portion of the value of his work, while said protective legal framework also caters for the need of the general public to enjoy the fruits of a robust, rich, and sufficiently protected public domain from the "information capitalism", which denigrates the value of intellectual commons and promotes the hyper-thick protections of current copyright law<sup>98</sup>. The WIPO Development Agenda<sup>99</sup> adheres to a protectionist approach of the public domain. In its Recommendation 16 advocates to "consider the preservation of the public domain within WIPO's normative processes and deepen the analysis of the implications and benefits of a rich and accessible public domain". Also, WIPO's Recommendation 20 intends to "promote norm-setting activities related to IP that support a robust public domain in WIPO's Member States, including the possibility of preparing guidelines which could assist interested Member States in identifying subject matters that have fallen into the public domain within their respective jurisdictions". WIPO's adherence to protect public domain indicates an international trend in motivating both national and international policymakers to focus on the definition of the public domain as well as to include provisions in law which cater for the protection and promotion of places of non-exclusive intellectual property rights<sup>100</sup>.

---

97. Spinello R., and Bottis, M., (2009), *ibid*, p. 6. The authors compare 'normative individualism' or 'information capitalism' with 'information socialism' with the aim to ponder on Locke, Fichte, and Hegel's theories for an author's moral right to appropriate the value of his/her creative expression without causing any direct harm to the intellectual commons. The authors contend that Locke's theory is especially helpful in reconciling strong intellectual property rights with a commons composed of intangible goods.

98. Spinello R., and Bottis, M., (2009), *ibid*, p. 10.

99. See *The 45 Adopted Recommendations under the WIPO Development Agenda* which in 2007 the General Assembly of WIPO Member States adopted (45 out of the 111 original proposals). The 45 adopted recommendations are available at <<http://www.wipo.int/ip-development/en/agenda/recommendations.html>> [last check, Apr. 20, 2011].

100. Dusollier, S., (2010), *ibid*, p. 5, who considers that protection of the public domain comprises of two steps: 1) identifying the contours of the public domain, thereby helping to assess its value and realm, and 2) considering and promoting the conservation and accessibility of the public domain. See, also, Sherman, B., and Wiseman, L., (2006), *ibid*, p. 260 in

## Archives in the public domain in Greek Legislation

Is the public domain, or any notion of it in law, sufficiently provisioned and protected in the Greek Copyright Law?

Legislation in effect currently in Greece, which includes provisions catering for works in the commons, is legislation that defines and regulates the creation, availability, distribution and permitted use of archives which are (supposed to be) available for use in the public commons. Law 1946/1991 gives the definition for the meaning of an archive and determines the new legal framework ruling the operation of the General State Archives<sup>101</sup> organization up to date. The Central Service of the General State Archives organization is composed of departments, and archives are established in the capitals of the Prefectures that did not exist in the past. Article 1 of Law 1946/1991 provides the definition for the meaning of an archive described as the collection of records and documents, no matter what the imprinted or implied dating of the record and/or document is as well as the size and material of it, which (record and/or document) may be related to the authorities of State, public or private organizations or legal entities or physical persons or a group of physical persons<sup>102</sup>. Further articles of the same Law provide the definitions for public<sup>103</sup>, ecclesiastical<sup>104</sup>, and private<sup>105</sup> archives as well as the definition for audiovisual<sup>106</sup> archives and archives of maps and drawings<sup>107</sup>.

In the Greek law there has been no classification of archives similar to the categorization of government information provided in other European countries' legislation such as in Dutch policy for improving access to public sector information.

---

which WIPO is reported to have said that a robust public domain, rather than being the antithesis of copyright protection, is the foundation upon which the copyright system works. It is the availability of public domain resources that enables exchange and creativity.

101. The *General State Archives (G.S.A.)* is a centre of national heritage and its main goal is to protect and preserve Greek historical memory. Through this new portal at <<http://www.gak.gr/frontoffice/portal.asp?cpage=NODE&cnode=1&clang=1>> [last check, Apr. 20, 2011].

102. See, also, Law 2846/2000 which refers to the Archives of the Prime Minister.

103. See article 2 of Law 1946/1991.

104. See article 3 of Law 1946/1991.

105. See article 4 of Law 1946/1991.

106. See article 5 of Law 1946/1991.

107. See article 6 of Law 1946/1991.

Dutch government information is categorized as research data<sup>108</sup>, public registers<sup>109</sup>, administrative data<sup>110</sup>, and auxiliary data<sup>111</sup>.

All laws pertaining to archives and their availability in the public domain-the commons-in Greece make provisions for the public's right to access and use them on condition of due respect to any applicable intellectual property rights. In other words, access of works aimed to become available in the public domain is provisioned only as conditional in the Greek law; in case of effective copyright or industrial property restraints, the general public's right to access and make use-even merely the non-transformative and passive use of reading-of any kind of records and/or documents and/or any other material that is defined as an archive, and which theoretically, at least, should have been available for the general public and accessible in the commons falters because of intellectual or industrial property rights<sup>112</sup>.

The same reasoning in the provisions of law is identified to the more recently passed legislative texts such as the so called "*Translucence Program*" that was passed through Law 3861/2010 and which requires the publication of any action or decision of a public sector organization<sup>113</sup> or decision-making body onto

---

108. Research data comprises the information collected by public organization, the key task of which is to collect data for use by others. The primary customers of these organizations are different parts of government which use the data in policymaking and administration. See Eechoud, van M., (2006), *The commercialization of public sector information: delineating the issues*, Chapter XII in Lucie Guibault and P. Bernt Hugenholtz (eds.) *The future of the public domain – identifying the commons in information law*, Kluwer Law International, pp. 279-301.

109. Public register data covers the public registers that are held on the basis of specific laws and regulations. See Eechoud, van M., (2006), *ibid*.

110. Administrative data results from the exercise of a particular administrative task of a public sector body that is directly aimed at citizens or companies. These include tax registers, police registers, social security files, etc. See Eechoud, van M., (2006), *ibid*.

111. Auxiliary data comprises information not belonging to any of the above categories. This data is collected and enhanced to support policymaking or the execution of government policies. See Eechoud, van M., (2006), *ibid*.

112. See article 5§5 of Law 2690/1999; see, also, article 1§2(b) of *Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information*, *Official Journal L 345*, 31/12/2003 P. 0090 – 0096, available at <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0098:EN:HTML>> [last check, Apr. 20, 2011], according to which said Directive shall not apply to documents for which third parties hold intellectual property rights.

113. The meaning of the "Public Sector Organization" is derived from article 2§§1,2,3 of Law 3861/2010 according to which (1)- The provisions of this Act apply to laws, decrees, decisions and acts of the Prime Minister, the Cabinet and collective government bodies, Minis-



the Internet.<sup>114</sup> More precisely, effective copyright restraints result in the failure of the general public's right to access and make use of public administration's works in the public domain regarding the availability of said works in the online environment of the commons.

---

ters, Deputy Ministers, Deputy Ministers, Secretary Generals of Ministries and Prefectures, Special Secretaries to Ministries, administrative bodies of public law entities (public entities), the independent regulatory authorities, the State Legal Council, the governing bodies of institutions of the public sector in the cases referred to in this Act, and the entities of the local authorities of first and second grade. The provisions of this Law shall also apply to acts or decisions issued by entities, to which the referred to in this paragraph institutions have granted authority to sign or delegate responsibility. (2)- For the purposes of this Act as agents of the public sector are meant: a) private entities owned or sponsored regularly in accordance with the applicable provisions of state funds at least 50% of the annual budget and b) public companies and organizations referred to in Article 1 of Law 3429/2005. (3)- For the purposes of this Act as agents of local government of first and second grade are meant the elected officers of Local Authorities (OTA) first and second grade and legal persons and enterprises of local authorities. In a number of rulings such as Case C-360/96 BFI Holding [1998] ECR I-6821, Case C-44/96 Mannesmann v. Strohalm [1998] ECR I-73, Case C-214/00 Commission v. Spain [2003] ECR I-4667, Case C-373/00 Adolf Trully [2003] ECR I-1931, and Case C-18/01 Korhonen [2003] ECR I-5321, the European Court of Justice (ECJ) has clarified that a "Public Sector body" includes organizations under both public and private law which are established for specific purpose of meeting needs in the general interest not having an industrial or commercial character, i.e. needs that are satisfied otherwise than by the supply of goods and services in the marketplace and which, for reasons associated with the general interest, the State chooses to provide itself or over which it wishes to retain a decisive influence. Said organizations must possess a legal personality and must be closely dependent as regards financing, management or supervision on the State, regional or local authorities or other bodies governed by public law. See, also, the definition of the "Body governed by Public Law" in article 1(b) of Directive 93/37/EEC OJ 1993 L 199/54 concerning the coordination of procedures for the award of public works contracts, available at <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0037:EN:NOT>> [last check, Apr. 20, 2011] as well as article 1(b) of Directive 92/50/EEC OJ 1992 L 209/1 relating to the coordination of procedures for the award of public service contracts, available at <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31992L0050:EN:NOT>> [last check, Apr. 20, 2011].

114. See article 5 of Law 3861/2010, the so called Translucence Program (*Πρόγραμμα Διαύγεια*) available at <[http://www.epdm.gr/Uploads/Files/nomoi\\_kya/N\\_3861\\_2010.pdf](http://www.epdm.gr/Uploads/Files/nomoi_kya/N_3861_2010.pdf)> [last check, Apr. 20, 2011], which makes room for the nullification of translucence of any action/decision of a public sector authority through the publication of relevant documentation onto the Internet, in the event of effective third-party's intellectual or industrial property rights. See, also, Law 3861/2010's Preamble, p. 5, available at <<http://diavgeia.gov.gr/site/AITIOLOGIKIEKTHESI2.pdf>> [last check, Apr. 20, 2011].

For any offline availability in the commons of said works, such as the physical environment of public libraries or other public archives, current legislation in Greece though it sets conditions for legitimate access and proper use, it is not prohibitive at least for the passive use of these works. It does not prohibit access and passive use, i.e. accessing and mere reading of protected works that become available in the restricted physical environment of public libraries or public archiving organizations such as the General State Archives or other Government organizations' libraries and/or archiving repositories. The passive act of reading is not regulated by copyright law, and the act of accessing archives in the commons of the restricted physical environment of public libraries or public archiving organizations cannot be understood as a violation of relevant law<sup>115</sup>. If this is true for the offline environment, it is also true for the online. Yet, it seems that Greek Copyright Law treats both truths differently.

The different treatment in Greek Copyright Law as well as in laws catering for the archives of works in the online public domain compares to works in the offline public domain provides sufficient evidence that currently there is a senseless imbalance in legislation in Greece to the detriment of the public domain, especially the digital public domain, which current public administration in Greece seems to aim at enhancing and enriching directly or indirectly through legislation such as Law 3861/2010. Said imbalance, which favours the offline availability of works in the public domain while at the same time discriminates against an equivalent availability of the same works in the online public domain, is the result of legislation that was formed and passed without any proper or thorough consideration for the evolution of Internet networking technologies and their catalytic effects on intellectual and industrial property rights as well as on the general public's rights for works in the public domain.

The fact that Greek legislation caters for works in the public domain and makes provisions for the public's right to access and use them on condition of due respect to any applicable intellectual or industrial property rights, indicates also that the notion of the public domain per se in the Greek legislation is the so called "*traditional*" one, according to which the public domain is defined as encompassing intellectual elements that are not protected by copyright or whose protection has lapsed due to the expiration of the duration of the copyright protection. Succumbing to that traditional mind-frame of Greek legislation is the rule, and the

---

115. Kallinikou, D., (2010), *Intellectual property, digital archives, and the public domain*, speech to Hellenic National Audiovisual Archive, Sep.20, 2010, available at <[http://www.avarchive.gr/files/Image/Kallinikou\\_30%20-9-2010.pdf](http://www.avarchive.gr/files/Image/Kallinikou_30%20-9-2010.pdf)> [last check, Apr. 20, 2011]; Dusollier, S., (2010), *ibid*, p. 8.

pass of Law 3861/2010 is not an exception to the rule. Such notion is negative, as its realm is the inverse of the scope of copyright protection.

The negative approach to public domain entails that if copyright is regulated and promoted, then the elements of public domain themselves are generally not subject to any rules or protection<sup>116</sup> or that any rules that might exist governing the public domain and/or ruling for any obligation or right with the aim to enrich and enlarge the public domain with works produced either by public or private bodies succumb to regulation for copyright protection. Neither is this definitely a positive view for public domain protection, nor a bold step towards the unhindered access of the general public in works supposedly to be in the public domain! And it reminds a lot, a description of public domain that was attempted by UNESCO in its “2003 Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace,” according to which “public domain information is publicly accessible information, the use of which does not infringe any legal right, or any obligation of confidentiality. It thus refers on the one hand to the realm of all works or objects of related rights, which can be exploited by everybody without any authorization, for instance because protection is not granted under national or international law, or because of the expiration of the term of protection. It refers on the other hand to public data and official information produced and voluntarily made available by governments or international organizations”<sup>117</sup>. The right approach, though, to public domain’s nature is to understand it not as the realm of material that is undeserving of protection, but as a device that permits the rest of the copyright system to work by leaving the raw material of authorship available for authors to use<sup>118</sup>.

In addition, the striking difference in the treatment provisioned in the Greek law of the offline and online environments of the public domain is characteristic in the application of legal restrictions stemming from copyright for protected works in the Internet, while no such application is usually exercised by right-holders in the environment of public libraries and archiving repositories. And this happens, despite the fact that copyright pertains only to the intangible work which is distinguished from the material property in which the protected work has been embodied<sup>119</sup>. In both environments, the online and offline, wherein protected works

---

116. Dusollier, S., (2010), *ibid*, p. 7.

117. UNESCO, (2003), *Recommendation concerning the promotion and use of multilingualism and universal access to cyberspace*, Adopted by the UNESCO General Conference in 2003 (32<sup>nd</sup> session), available at <[http://portal.unesco.org/ci/en/ev.php-URL\\_ID=13475&URL\\_DO=DO\\_TOPIC&URL\\_SECTION=201.html](http://portal.unesco.org/ci/en/ev.php-URL_ID=13475&URL_DO=DO_TOPIC&URL_SECTION=201.html)> [last check, Apr. 20, 2011].

118. Litman, J., (1990), *ibid*, p. 968.

119. Kallinikou, D., (2008), *ibid*, pp. 30-34.

become available they are available for “public performance”, “communication to the public” and probably for “broadcasting”, too.

Greek Copyright Law considers “public performance” as any performance of a work at a place where the public is or can be present, or at a place not open to the public, but where a substantial number of persons outside the normal circle of a family and its closest social acquaintances are present<sup>120</sup>. The availability of a work in the offline environment of a public library as well as in the online environment of the Internet meets the “public performance” criterion in copyright law. On the basis of the right of public performance, the author or any other right-holder may authorize live performances of a work, such as the presentation of a play in a theatre or an orchestra performance of a symphony in a concert hall etc. Public performance also includes performance by means of recordings; thus, musical works embodied in phonograms are considered “publicly performed”, when the phonograms are played over amplification equipment in such places as libraries.

In addition, the right of “broadcasting” covers the transmission by wireless means for public reception of sounds or of images and sounds, whether by radio, television, or satellite.<sup>121</sup> When a work is “communicated to the public”<sup>122</sup> a signal is distributed, by wire or wireless means, which can be received only by persons who possess the equipment necessary to decode the signal. An example of “communication to the public” is cable transmission or transmission of a work via the

---

120. Kallinikou, D., (2008), *ibid*, pp. 163-177. See also article 3§2 of Law 2121/1993 available at <<http://web.opi.gr/portal/page/portal/opi/info.html/law2121.html/ch01.html#a3>> [last check, Apr. 20, 2011] according to which The use, performance or presentation of the work shall be deemed to be public when the work thereby becomes accessible to a circle of persons wider than the narrow circle of the family and the immediate social circle of the author, regardless of whether the persons of this wider circle are at the same or at different locations. Greek Court decisions upon the nature of public performance of a work include Supreme Court (ΑΠ) 135/1983 ΕλλΔικ 1983 pp. 1332-1333, ΑΠ 61/1981 ΝοΒ 1981 pp. 384-385, ΑΠ 64/1984 ΠοινΧρ 1984 pp. 705-706, ΑΠ 500/2001 ΕλλΔ 2001 p. 847, ΑΠ 433/1992 ΕΕμΔ 1994 p. 293 & ΕλλΔ 1993 p. 1411, & ΠοινΧρ 1992 pp. 534-535, ΑΠ 907/2003 ΠοινΧρ 2004 pp. 213-215 & ΕλλΔ 2003 pp. 1480-1481; also, First Instance Court decisions 67230/1976 ΝΔ 1976 pp. 470-472 & ΝοΒ 1977 pp. 789-790 & ΑpxN 1977 pp. 61-62 & ΠοινΧρ 1977 pp. 279-280 & ΕΕμΔ 1977 pp. 136-139, First Instance Court of Athens 5808/2002, First Instance Court of Athens 1577/2003, Athens Three-member Criminal Court 29171/1975 ΠοινΧρ 1976 pp. 773-774, First Instance Court of Athens 3413/2002 ΧρΙΔ 2003 pp. 652-654, First Instance Court of Athens 1639/2001 ΔΕΕ 2001 pp. 858-860.

121. See article 3§1(g) of Law 2121/1993, available at <<http://web.opi.gr/portal/page/portal/opi/info.html/law2121.html/ch01.html#a3>> [last check, Apr. 20, 2011]; Kallinikou, D., (2008), *ibid*, pp. 177-183.

122. See Kallinikou, D., (2008), *ibid*, pp. 161-163.

intranet of a public library. The difference between the right to communicate a work to the public<sup>123</sup> and the right to a public performance<sup>124</sup> of a work is that in the case of the former the public is not present at the place where the communication originates from, while in the case of the later it is<sup>125</sup>. Under the Berne Convention<sup>126</sup>, authors have the exclusive right of authorizing public performance, broadcasting and communication to the public of their works. In Greece, provisions for safeguarding said rights for the author/right-holder are also included in Copyright Law 2121/1993 in Greece<sup>127</sup>.

The striking difference in the treatment in law of the offline and online environments of the public domain stems from the fact that copyright law restrictions are almost always claimed by right-holders and become acceptable by courts regarding the unauthorized availability of their works online, while no such claims are raised regarding the availability of works in the commons of the offline environment of public libraries and archiving organizations. Non-transformative uses of works such as accessing and reading them through the non-traditional online environment seem to collide with traditional copyright law provisions<sup>128</sup>. The mere accessing and reading of a book that becomes available online, even if said actions are taken for non-commercial purpose might be in breach of copyright law which confers the author with the exclusive right to authorize or prohibit the fixation and direct or indirect, temporary or permanent reproduction of his/her

---

123. See article 3§1(h) of Law 2121/1993.

124. See article 3§1(f) of Law 2121/1993.

125. See Recital 23 of the *InfoSoc Directive* available at <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML>> [last check, Apr. 20, 2011]; Kallinikou, D., (2008), *ibid*, pp. 161-163; see also *MovΠρωτΑθ 3413/2002 XpΙΔ 2003*, pp. 652-654; *MovΠρωτΑθ 1639/2001 ΔΕΕ 2001*, pp. 858-860.

126. See article 11bis of the *Berne Convention*, **available at** <[http://www.wipo.int/treaties/en/ip/berne/trtdocs\\_wo001.html#P156\\_28886](http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html#P156_28886)> [last check, Apr. 20, 2011] titled *Broadcasting and Related Rights 1) Broadcasting and other wireless communications, public communication of broadcast by wire or rebroadcast, public communication of broadcast by loudspeaker or analogous instruments; 2) Compulsory licenses; 3) Recording; ephemeral recordings. See the Berne Convention of September 9, 1886, and its amendments ever since for the Protection of Literary and Artistic Works, available at* <[http://www.wipo.int/treaties/en/ip/berne/trtdocs\\_wo001.html](http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html)> [last check, Apr. 20, 2011].

127. See article 3 of Law 2121/1993, available at <<http://web.opi.gr/portal/page/portal/opi/info.html/law2121.html/ch01.html#a3>> [last check, Apr. 20, 2011].

128. See Court of First Instance decisions *MovΠρωτΑθ 3413/2002 XpΙΔ 2003* pp. 652-654, *MovΠρωτΑθ 1639/2001 ΔΕΕ 2001* pp. 858-860.

works by any means and in any form, in whole or in part<sup>129</sup>. The author is also conferred with the exclusive right on the public performance of his/her works, the broadcasting or rebroadcasting of his/her works to the public by radio and television by wireless means or by cable or by any kind of wire or by any other means, in parallel to the surface of the earth or by satellite, the communication to the public of his/her works by wire or wireless means or by any other means, including the making available to the public of his/her works in such a way that members of the public may access these works from a place and at a time individually chosen by them. These exclusive rights of the author are not exhausted by any act of communication to the public<sup>130</sup>.

The copyright protection of traditional legal frameworks seems to prohibit even non-transformative uses of works online, even if said uses are made with non-commercial interest<sup>131</sup>. Copyright law seems to impede end-users even from engaging in the most inoffensive non-transformative uses of creative works such as reading a work online and via their computers, unless they ask for prior permission from the author and/or right-holder of the right to access to and copying of protected works. Every time the users are accessing copyrighted works that are available online via their computers, they have no option but to copy the said works in order to use them. Said copying is done without any prior permission from the author and/or right-holder, and unless said copying is permitted as an exception from the reproduction right of the author and/or right-holder<sup>132</sup>, violation of copyright is the outcome. Therefore, existing copyright system does not encourage users to make confident and lawful use of works available onto the In-

---

129. See article 3§1(a) of Law 2121/1993, available at <http://web.opi.gr/portal/page/portal/opi/info.html/law2121.html/ch01.html#a3> [last check, Apr. 20, 2011].

130. See article 3§§1(f), (g), (h) of Law 2121/1993.

131. Stallman, R., (2002), *The right to read, in free software free society: selected essays of Richard Stallman*, GNU Press, Boston, p. 73; see also, the same, (1997), *The right to read*, 40 Communications of the ACM, 2, available at <<http://www.gnu.org/philosophy/right-to-read.html>> [last check, Apr. 20, 2011], who, by projecting current trends in copyright law, sets a fictional story in 2047 and pictures a world in which access to information is strictly controlled and is deployed by 'trusted' computing systems only. In said fictional world, no one is allowed to read another's book without a license, and each book has a copyright monitor which reports when, where, who read a book to a hypothetical central authority.

132. See article 28B of Law 2121/1993, according to which Temporary acts of reproduction which are transient or incidental, which are an integral and essential part of a technological process and whose sole purpose is to enable: a) a transmission in a network between third parties by an intermediary or b) a lawful use of a work or other protected subject-matter, and which have no independent economic significance, shall be exempted from the reproduction right.

ternet. Even the most inoffensive non-transformative uses of creative works such as reading a work online or downloading a work with the aim to read it privately without any commercial purpose in mind is considered by courts as an action that conflicts with a normal exploitation of the work or other protected subject-matter and unreasonably prejudices the legitimate interests of the rightholder, according to existing copyright Law provisions and according to the application of the “three-step-test”<sup>133</sup>.

This treatment of users’ online behaviour by currently effective Copyright legislation in Greece does not make any balanced sense and cannot achieve any equilibrium between an author’s proprietary rights and the general public’s right to access and read an author’s output, as this equilibrium was conceived both through the Lockean and Kantian perspectives for intellectual property. The difference in the treatment of actions such as accessing and reading of a work depending whether these actions take place offline or online beefs up the argument that the existing legal framework for Copyright-in Greece as in elsewhere, too-cannot cope successfully with the online environment of digitized works and discriminates clearly against any online public domain operation.

### Voicing the need for Copyright reform

A functioning copyright system must provide the incentives needed for creative professionals, but must also protect the freedoms necessary for scientific research and amateur creativity to flourish. In this scope and regarding the digital environment, copyright seems to have failed at both<sup>134</sup>. And this failure is not the outcome of local or national copyright policy, but rather it is the result of international decision-making in intellectual property regulation; it is the result of lagging rule-making and of sluggish provisions in international intellectual property conventions. Voices supporting action for copyright reform at the international level are becoming more and are sounding louder by the pass of time.

---

133. See article 28C of Law 2121/1993, available at <<http://web.opi.gr/portal/page/portal/opi/info.html/law2121.html/ch04.html#a28c>> [last check, Apr. 20, 2011].

134. Kaitlin, M., (2010), *Lessig calls for WIPO to lead overhaul of copyright system*, Intellectual Property Watch, available at <[http://www.ip-watch.org/weblog/2010/11/05/lessig-calls-for-wipo-to-lead-overhaul-of-copyright-system/?utm\\_source=post&utm\\_medium=email&utm\\_campaign=alerts](http://www.ip-watch.org/weblog/2010/11/05/lessig-calls-for-wipo-to-lead-overhaul-of-copyright-system/?utm_source=post&utm_medium=email&utm_campaign=alerts)> [last check, Apr. 20, 2011]; Lawrence Lessig questioned the survivability of current Copyright system as it was designed and has been inherited from the past. For Lessig, The copyright system will never work on the Internet. It’ll either cause people to stop creating or it’ll cause a revolution. Lessig cited a growing system of copyright “abolitionism” online in response to a worrying tendency to criminalize the younger generation.

The copyleft movement and the licensing of works that has been developed because of and through it is the most characteristic voicing for copyright reform leveraging on existing copyright regulation. Licensing one's work under a copyleft license, such as a Creative Commons license, does not amount to the relinquishment of copyright, but rather amounts to an exercise of intellectual property rights provisioned through existing regulation. Based on licenses granting the right to copy, distribute, communicate, and modify the licensed work, Creative Commons licensing pursues similar-yet not identical-objectives to the public domain, i.e. the promotion of free availability, use, and exploitation of licensed works set under certain conditions for such availability, use, and exploitation. In that sense, Creative Commons licensing-and any other copyleft licensing-ends up in the creation of a sort of public domain, born from within the monopoly and exclusivity of copyright. Said licensing enables creating a sphere of free use of licensed works without giving up the author's exclusivity owned because of effective copyright<sup>135</sup>.

Copyleft and Open Access movements purport to enhance ideologically the existence and further development of the public domain. Both movements represent a copyright reform initiative that subverts copyright from within, and cause a normative change in the way intellectual property rights are exercised aiming at the reconstitution of the balance between an author's intellectual property rights and the general public's interest in accessing and using creative expressions<sup>136</sup>. The search of the said balance becomes also explicit in the "2004 Geneva Declaration on the Future of the World Intellectual Property Organization"<sup>137</sup>. It has been widely questioned through the noteworthy work of many poised scientists and copyright theorists, too<sup>138</sup>.

Given that the public domain is not sufficiently provisioned and protected in the Greek Copyright Law, what needs to be done?

---

135. Dusollier, S., (2010), *ibid*, p. 52.

136. Dusollier, S., (2010), *ibid*, p. 52.

137. WIPO, (2004), Geneva declaration on the future of the World Intellectual Property Organization, available at <http://www.cptech.org/ip/wipo/genevadeclaration.html> [last check, Apr. 20, 2011].

138. See Boyle, J., (2004), *Manifesto on WIPO and the Future of Intellectual property*, 9 Duke Law and Technology Review, available at <<http://www.law.duke.edu/journals/dltr/articles/2004dltr0009.html>> [last check, Apr. 20, 2011]; Reichman, J., and Maskus, K., (2004), *The globalization of private knowledge goods and the privatization of global public goods*, 7 Journal of International Economic Law, 2, pp. 279-320, available at <<http://www.law.duke.edu/cspd/articles/reichman.pdf>> [last check, Apr. 20, 2011]; Signed-on July 7, 2003, letter from 69 scientists and economists to Kamil Idris, Director General of the World Intellectual Property Organization requesting that WIPO host a meeting on open and collaborative development, available at <<http://www.cptech.org/ip/wipo/kamil-idris-7july2003.pdf>> [last check, Apr. 20, 2011].



What is still missing in the Greek copyright system and what needs to be done is an amendment in Copyright Law aiming at the positive protection of the public domain that could protect it against either privatisation of its elements or unequal legal support compares to the provisions of law that cater for copyright protection. In France, some scholars<sup>139</sup> have started to develop a positive protection for the public domain on the civil law notion of “les choses communes” or the commons appearing in article 714 of the French Civil Code<sup>140</sup>. The positive description of the public domain in law is a legislative proof that public domain plays an essential role for cultural and democratic participation, economic development, education and cultural heritage. Aligning the private domain of exclusivity and the public domain of collective use within one regime of intellectual property is the way to describe in law the balance of interests embedded in copyright laws that cater for both the right-holders of intellectual property as well as the general public’s interests in copyrighted or not copyrighted work<sup>141</sup>. The lack of a positive description in law for public domain as well as the negative definition of public domain in legislation as the reverse of copyright is an evidence of an imbalance in law concerning the protection from one side of author’s exclusive rights and from the other of general public’s interests in creative works. The Greek copyright law is still imbalanced and lagging in passing a positive description in its provisions for public domain acknowledgement, protection, and enhancement.

Greek Copyright Law 2121/1993 does not include any provisions for positive acknowledgement, protection, and enhancement of the public domain, with the exception of article 29§2, which pertains to the duration of copyright protection and describes State’s empowerment to pursue, after the expiration of copyright’s term of protection, the protection of a work’s integrity stemming from an author’s moral rights that are inalienable and beyond any expiration<sup>142</sup>. Yet, this is

139. Choisy, S., (2002), *Le domaine public en droit d’auteur*, No 22, Litec -Editions du Juris Classeur; Chardeaux, M.A., (2006), *Les Choses Communes*, LGDJ; Dusollier, S., (2010), *ibid*, p. 67.

140. Article 714 in Book III of the French Civil Code pertaining to the various ways in which ownership is acquired provides that There are things which belong to nobody and whose usage is common to all. Public order statutes regulate the manner of enjoying them. The text in French is Il est des choses qui n’appartiennent à personne et dont l’usage est commun à tous. Des lois de police règlent la manière d’en jouir.

141. Dusollier, S., (2007), *Sharing access to intellectual property through private ordering*, 82 Chicago-Kent Law Review, 3, p. 1932, available at <<http://www.crid.be/pdf/public/5610.pdf>> [last check, Apr. 20, 2011].

142. See article 29§2 of Law 2121/1993, according to which After the expiry of the period of copyright protection, the State, represented by the Minister of Culture, may exercise the rights relating to the acknowledgment of the author’s paternity and the rights relating

not a positive provision in law concerning the public domain. And neither can it guarantee the free use of unprotected elements of works that fall in the public domain when their copyright has expired nor can it immunize them against any reservations or exclusivity either by intellectual property rights through the recapture of copyright or by any technological measures<sup>143</sup>. Greek Copyright Law's provisions provide no balancing counter-measures to any contractual or technical private measures, which aim at enforcing unilaterally right-holder's intellectual property rights by locking up works either copyrighted or in the public domain preventing any use of them either it is included in the exceptions and limitations of Copyright Law or not. The main consequence of such private initiatives is to cause a shift from the intended in law balance to a unilaterally determined norm of usage of intellectual property rights<sup>144</sup>.

The positive description of the public domain in law should immunise the public domain from any encroachment or appropriation of its elements. It should affirm through new provisions of copyright law the prohibition of a recapture of a work as a whole that resides in the public domain, as well as guarantee the collective use of work fallen into the public domain in the sense that anyone from the general public is entitled to use, modify, exploit, reproduce, and create new works

---

to the protection of the integrity of the work deriving from the moral rights pursuant to Article 4(1)(b) and (1)(c) of this Law. The provision of article 29§2 of Law 2121/1993 is similar to France's article L. 122-9 CPI which provides that the Minister of Culture can refer to the court of first instance a case of abuse in the exercise of the right of divulgation even for works in the public domain. The Minister of Culture can claim in the courts the respect of the moral right of the author either said claim relates to a violation of the divulgation of the work or to the refusal for divulgation. That means that the provision for the intervention of the Minister of Culture is not limited to any act of violation of the divulgation but extends also to any act that results in the refusal of the divulgation of the work; thus the Minister of Culture is empowered with the right to pursue in courts the protection of the an author's moral right by claiming the illegality of the refusal (probably claimed by the heirs or other subsequent right-holders of the author) of divulgation of an author's work that resides in the public domain if there's public interest at stake. See more, Dusollier, S., (2010), *ibid*, p. 39, as well as her reference in p. 40 to a famous case upon this issue that occurred in France with the Hugo's work *Les Misérables*; in said case, one of Hugo's heirs tried to prevent the publication of a sequel of his novel based on claims from moral right. The claim was ultimately denied by the court on the ground that a work fallen into the public domain was open for adaptation in respect of the freedom for creation. The court ruled that the moral right could only be invoked to protect the right of paternity and integrity but upon the sole condition that an actual harm to such rights was evident from the adaptation which the Hugo's heir tried to prevent.

143. Dusollier, S., (2010), *ibid*, p. 70.

144. Dusollier, S., (2007), *ibid*, p. 1394.

from works residing in the public domain<sup>145</sup>. A positive description of the public domain in law should operate conversely to the exclusivity and rivalry operations of the copyright being the explicit ground for non-exclusivity and non-rivalry, i.e. being the explicit description in law of the commons whose wealth lies in collective and non-rivalrous use and in the absence of any appropriation<sup>146</sup>. In the same sense, Greek Copyright Law needs to amend so as to enrich its provisions with allowances for non-commercial use of works online beyond the existing provisions of article 18<sup>147</sup>.

Traces of such a positive stance in case-law concerning the protection of the public domain have already been found in the European Court of Justice<sup>148</sup>, thus there is probably good timing for an amendment in Greek Copyright Law favouring such a positive description of the public domain. The positive description in copyright law could prohibit any action that may consist of knowingly performed reproduction, distribution, making available or communication to the public of a

---

145. Dusollier, S., (2010), *ibid*, p. 68.

146. Dusollier, S., (2010), *ibid*, p. 70.

147. See article 18 titled Reproduction for Private Use according to which (1) Without prejudice to the provisions laid down in the following paragraphs, it shall be permissible for a person to make a reproduction of a lawfully published work for his own private use, without the consent of the author and without payment. The term private use shall not include use by an enterprise, a service or an organization. (2) The freedom to make a reproduction for private use shall not apply when the act of reproduction is likely to conflict with normal exploitation of the work or to prejudice the author's legitimate interests, and notably: a) when the reproduction is an architectural work in the form of a building or similar construction, b) when technical means are used to reproduce a fine art work which circulates in a restricted number of copies, or when the reproduction is a graphical representation of a musical work.

148. See Opinion of the Advocate General Ruiz Jarabo Colomer, October 24, 2002, in the Linde case, in joined cases C-53/01 (Linde AG), C-54/01 (Winward industries Inc.), and C-55/01 (Radio Uhren AG), regarding the interpretation of Article 3(1)(b), (c) and (e) of First Council Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks (OJ 1989 L 40, p. 1); The Advocate General has held that the public interest should not have to tolerate even a slight risk that trade mark rights unduly encroach on the field of other exclusive rights which are limited in time whilst there are in fact other effective ways in which manufactures may indicate the origin of a product. Said Opinion relates to ECJ Decision of April 8, 2003, that is available at <<http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79969591C19010053&doc=T&ouvert=T&seance=ARRET>> [last check, Apr. 20, 2011]. Dusollier, S., (2010), *ibid*, pp. 50, 69; Laustsen, R.D., (2009), *The principle of keeping free within EU Trade Mark Law*, available at <http://www.marques.org/teams/LGMS/2009%20Rasmus%20Laustsen.pdf> [last check, Apr. 20, 2011].

work belonging to the public domain under a name that is not the one of the real author. It could also prohibit any action which may be based upon fraudulently claims of economic rights in a work belonging to the public domain. Provisions with this suggested content in Greek Copyright Law would sanction any attempt of encroachment of works belonging to the public domain as well as any attempt either through private contracts or technical means to regain exclusivity of a work belonging to the public domain. The said provisions could set unsanctioned by law any attempt to set up remuneration fee for the provision of public domain content, in case the “domaine public payant” managed to implement<sup>149</sup>.

The said recommended provisions as an amendment to Greek Copyright Law require the adoption of normative rules in intellectual property legal framework and the setting up of material conditions which could effectively enable access to and enjoyment, and preservation of the public domain. The suggested amendment to Greek Copyright Law is necessary for robust public domain recognition in legislative text, which would create certainty in the identification of the composition of the public domain and works falling into it. It would, also, enhance the availability of the public domain materials, the effectiveness of access to them, and, thus, public domain’s sustainability. The suggested amendment in law should guarantee the application of the non-exclusivity principle for materials that reside in the public domain in the sense that the law should prohibit any commodification or private recapture of works residing in the public domain. The suggested amendment in law should, finally, guarantee the application of the non-rivalry principle for materials of the public domain in the sense that the absence of any exclusive rights upon the public domain materials entails an effective collective use of them without any discrimination<sup>150</sup>.

---

149. The implementation of the “domaine public payant” would render uninteresting the commercial exploitation of works in the public domain by any encroaching appropriator. See more, Dusollier, S., (2010), *ibid*, p. 69.

150. See Dusollier, S., (2010), *ibid*, pp. 70-71 who describes the four pivotal principles-1) certainty, 2) availability and sustainability, 3) non-exclusivity, and 4) non-rivalry-for a robust public domain, as they are stated in *The 45 Adopted Recommendations under the WIPO Development Agenda* which in 2007 the General Assembly of WIPO Member States adopted. Recommendation 20 of the WIPO Development Agenda speaks for promotion of norm-setting activities related to IP that support a robust public domain in WIPO’s Member States, including the possibility of preparing guidelines which could assist interested Member States in identifying subject matters that have fallen into the public domain within their respective jurisdictions. The 45 adopted recommendations are available at <<http://www.wipo.int/ip-development/en/agenda/recommendations.html>> [last check, Apr. 20, 2011].

# Online gambling and EU Law

---

---

Thomas Papadopoulos

---

---

## 1. Introduction

The regulation of online gambling plays a very important role in the area of internal market of European Union. Gambling in an online environment offers opportunities for cross-border economic activities. Internet has opened new ways in cross-border gambling activities. Gambling operators could easily offer gaming and betting services via Internet; consumers from other Member States get easy access to these gambling services through Internet.

This opening of the cross-border online gambling market has generated huge profits.

The annual revenues generated by the gambling service sector, measured on the basis of Gross Gaming Revenues (GGR) (i.e. stakes less prizes but including bonuses), were estimated to be around 75,9 bn € (EU 279) showing the economic significance of the sector. Online gambling services accounted for annual revenues in excess of € 6,16 bn, i.e. 7,5 % of the overall gambling market. This online market is the fastest growing segment and is expected to double in size in five years<sup>1</sup>. Nevertheless, this growth was not accompanied by legality and compliance. Many of these operators offered their services without complying with the national rules of their home or host Member State. These unauthorized, illegal providers constitute a vast problematic area of the internal market.

However, there are certain regulatory problems arising out of this expansion of cross-border gambling. Most of the national regulators are concerned with the following questions: “Who is going to regulate this cross-border activity?”, “Does the internal market of the European Union demands any regulatory reforms in the field of gambling?”, “Should Member States coordinate their actions and legislative choices in the area of gambling?”. In March 2011, the European Commission published its Green Paper on online gambling in the internal market. The purpose of this Green paper is to launch an extensive public consultation on all relevant public policy challenges and possible internal market issues resulting from the

---

1. EGBA and H2 Gambling Capital, 2009, [http://www.egba.eu/pdf/EGBA\\_FS\\_MarketReality.pdf](http://www.egba.eu/pdf/EGBA_FS_MarketReality.pdf) . COMMISSION STAFF WORKING PAPER, Accompanying document to the GREEN PAPER “On online gambling in the Internal Market” COM (2011) 128, 8.

rapid development of both licit and unauthorised online gambling offers directed at citizens located in the EU<sup>2</sup>.

## **2. Online gambling and Member States: regulatory problems at EU level**

With regard to gambling, Member States are interested in the regulation of this part of the internal market due to moral and social considerations (addiction etc.) and to budgetary reasons (e.g. profits for state-owned companies). In its Green Paper, the European Commission categorizes national legal regimes on online gambling. It finds out that there are two categories of national legal regimes: a) the first category of legal regimes is based on licensed operators providing services within a strictly regulated framework, and b) the second category is based on a strictly controlled monopoly (state-owned or otherwise)<sup>3</sup>.

These are two different regulatory models on online gambling which are responsible for the existence of a wide legal diversity among the various Member States. The various rulings of the European Court of Justice did not diminish this legal diversity. The European Court of Justice respected the national legal regimes on gambling. The regulatory autonomy of the Member States remained vastly untouched. The European Commission stress that, in the absence of harmonisation in the field of gambling, it is for each Member State to determine in those areas, in accordance with its own scale of values, what is required in order to ensure that the public interests are protected, in line with the subsidiarity principle. However, the European Court of Justice set a few criteria which national provisions should comply with.

The problem of legal diversity is aggravated by certain factors. First, the fact that online gambling activities could be cross-border adds another difficulty to both legal regimes. National legal orders are reluctant to accept online market operators originating from different Member States or from third countries outside the European Union. In this way, Member States quite often seek to defend their national monopolies or strict licensing systems. Secondly, the majority of online market operators across the Member States are illegal because they are operating without any license or accreditation. Out of 14,823 active gambling sites in

---

2. COMMISSION STAFF WORKING PAPER, Accompanying document to the GREEN PAPER "On online gambling in the Internal Market" COM (2011) 128, 3.

3. COMMISSION STAFF WORKING PAPER, Accompanying document to the GREEN PAPER "On online gambling in the Internal Market" COM (2011) 128, 3.

Europe more than 85% operated without any license<sup>4</sup>. Thirdly, the enforcement of national rules presents many defects. Diverse national rules with regard to gambling combined with these factors do not contribute to the establishment and smooth operation of a European common market for online gambling,

### **3. The purpose of the Green Paper on online gambling in the internal market**

As it was mentioned above, the purpose of this Green paper is to launch an extensive public consultation on all relevant public policy challenges and possible internal Market issues resulting from the rapid development of both licit and unauthorised online gambling offers directed at citizens located in the EU. The main objective of the Pan-European consultation is to explore the existing situation of the EU online gambling market.

The Commission is seeking detailed facts and views from all interested stakeholders on the existing situation of the EU online gambling market and the following key policy issues that the growth of this market gives rise to: a) the existence and extent of societal and public order challenges associated with online gambling; b) the regulatory and technical methods Member States use or could use to improve enforcement, consumer protection and the preservation of public order; c) the appropriateness and effectiveness of current rules applicable to online gambling services at EU level in terms of ensuring the overall coherence of national systems and evaluating whether further cooperation at EU level might assist Member States to achieve more effectively the objectives of their gambling policy<sup>5</sup>. Contributions to the consultation will determine the need for and form of EU follow-up action in this field, as well as the level at which such action should be taken. The objectives of the consultation are ultimately to achieve a market for online gambling services that is well-regulated for all<sup>6</sup>.

This public consultation is essential due to the regulatory and technical challenges described above and the different stances towards societal and public order is-

---

4. COMMISSION STAFF WORKING PAPER, Accompanying document to the GREEN PAPER "On online gambling in the Internal Market" COM (2011) 128, 3.

5. Public Consultation on Online gambling in the Internal Market - Frequently asked questions MEMO/11/186, p. 2.

6. Public Consultation on Online gambling in the Internal Market - Frequently asked questions MEMO/11/186, p. 2.

sues, such as the protection of consumers from fraud and the prevention of gambling addiction<sup>7</sup>.

#### **4. Online gambling and the case law of the European Court of Justice**

In many cases before case law was enacted, the European Court of Justice had the opportunity to examine the legal status of online gambling and sports betting in certain Member States. The regulation of online gambling plays a pivotal role in the area of internal market. This examination took place in the light of internal market. The European Court of Justice examined the relevant national provisions in the light of freedom to provide services and as well as freedom of establishment. In these cases, national gambling laws were challenged by private market participants who could not penetrate into the national gambling market of the Member State due to its strict licensing system or national monopoly. The European Court of Justice was called to adjudicate on the compatibility of these national laws on gambling with the EU fundamental freedoms. The most important parts of case laws which bear a significance for the European market of online gambling will be presented in the next paragraphs.

In Case C-67/98 *Zenatti*<sup>8</sup>, the European Court of Justice examined the transmission through internet or fax of sports betting. Mr Zenatti has acted as an intermediary in Italy for the London company SSP Overseas Betting Ltd ("SSP"), a licensed bookmaker. Mr Zenatti used to run an information exchange for the Italian customers of SSP in relation to bets on foreign sports events. He sent to London by fax or Internet forms which had been filled in by customers together with bank transfer forms, and received faxes from SSP for transmission to the same customers<sup>9</sup>.

The European Court of Justice found that this national law constitutes a trade barrier and inhibits the exercise of the fundamental freedom to provide services. However, this trade barrier which applied indistinctly to national and non-nationals could be justified in accordance with public interest requirements. The European Court of Justice stated that national legislation which reserves the right for certain bodies to take bets on sporting events and which thus prevents operators from taking bets in other Member States, directly or indirectly constitutes an obstacle to the freedom to provide services even if it applies without distinction.

---

7. Public Consultation on Online gambling in the Internal Market - Frequently asked questions MEMO/11/186, p. 2.

8. Case C-67/98 *Questore di Verona v Diego Zenatti* [1999] ECR I-7289.

9. Case C-67/98 *Questore di Verona v Diego Zenatti* [1999] ECR I-7289., para. 6.



However, in so far as such legislation does not entail any discrimination on grounds of nationality, it can be justified where its objectives are to protect consumers and to maintain order in society. Although it does not totally prohibit the taking of bets on sporting events but reserves this right for certain bodies under certain circumstances, determination of the scope of the protection which a Member State intends providing in its territory in relation to lotteries and other forms of gambling falls within the margin of appreciation enjoyed by the national authorities. It is for those authorities to appraise whether, in the context of the goal pursued, it is necessary to prohibit activities of this kind, totally or partially, or only to restrict them and to lay down more or less rigorous procedures for controlling them.

In those circumstances, the mere fact that a Member State has chosen a system of protection different from that adopted by another Member State cannot affect the appraisal as to the need for and proportionality of the provisions adopted. They must be assessed solely in the light of the objectives pursued by the national authorities of the Member State concerned and of the level of protection which they are intended to ensure<sup>10</sup>.

The ECJ concludes that the Treaty provisions on the freedom to provide services do not preclude national legislation, such as the Italian legislation, which reserves the right to certain bodies to take bets on sporting events if that legislation is in fact justified by social-policy objectives intended to limit the harmful effects of such activities and if the restrictions, which it imposes, are not disproportionate in relation to those objectives<sup>11</sup>.

Case C-243/01 *Gambelli*<sup>12</sup> is concerned again with the collection of bets on sporting events in one Member State and their transmission by internet to another Member State. This commercial activity was prohibited and this prohibition was enforced by criminal penalties imposed. The national legislation at issue reserved the right to collect bets to certain bodies. The European Court of Justice was called to scrutinize the compatibility of this national legislation with the freedom of establishment and the freedom to provide services. The European Court of Justice stated that national legislation which prohibits on pain of criminal penalties the pursuit of the activities of collecting, taking, booking and forwarding offers of bets, in particular on sporting events, without a licence or authorisation from the Member State concerned, constitutes a restriction on freedom of establish-

---

10. Case C-67/98 *Questore di Verona v Diego Zenatti* [1999] ECR I-7289., paras 29-36.

11. Case C-67/98 *Questore di Verona v Diego Zenatti* [1999] ECR I-7289., para 38.

12. Case C-243/01 *Criminal proceedings against Piergiorgio Gambelli and Others* [2003] ECR I-13031.

ment and on the freedom to provide services provided for in Articles 43 EC and 49 EC respectively, which, to be justified, must be based on imperative requirements in the general interest, be suitable for achieving the objective which they pursue, do not go beyond what is necessary in order to attain it and be applied without discrimination.

In this connection, it is for the national court to determine whether such legislation, taking account of the detailed rules for its application, actually serves the aims which might justify it, and whether the restrictions it imposes are disproportionate in the light of those objectives. In particular, in so far as the authorities of a Member State incite and encourage consumers to participate in lotteries, games of chance and betting to the financial benefit of the public purse, the authorities of that State cannot invoke public order concerns relating to the need to reduce opportunities for betting in order to justify measures such as those at issue in the main proceedings. Furthermore, where a criminal penalty was imposed on any person who from his home in a Member State connects by internet to a bookmaker established in another Member State, the national court must consider whether this constitutes a disproportionate penalty<sup>13</sup>.

In Joined Cases C-338/04, C-359/04 and C-360/04 *Placanica*, the European Court of Justice had the opportunity to examine the status of data transmission centers. The facts of this case involved Stanley International Betting Ltd. Stanley International Betting Ltd ('Stanley') is a company incorporated under English law and a member of the group Stanley Leisure plc ('Stanley Leisure'), a company incorporated under English law and quoted on the London (United Kingdom) stock exchange. Both companies have their head office in Liverpool (United Kingdom). Stanley Leisure operates in the betting and gaming sector and is the fourth biggest bookmaker and the largest casino operator in the United Kingdom<sup>14</sup>. Stanley is one of Stanley Leisure's operational conduits outside the United Kingdom. It is duly authorised to operate as a bookmaker in the United Kingdom by virtue of a licence issued by the City of Liverpool. It is subject to controls by the British authorities in the interests of public order and safety; to internal controls over the lawfulness of its activities; to controls carried out by a private audit company; and to controls carried out by the Inland Revenue and the United Kingdom

---

13. Case C-243/01 *Criminal proceedings against Piergiorgio Gambelli and Others* [2003] ECR I-13031, paras 65, 69, 72, 76.

14. Joined cases C-338/04, C-359/04 and C-360/04 *Criminal proceedings against Massimiliano Placanica (C-338/04), Christian Palazzese (C-359/04) and Angelo Sorricchio (C-360/04)* [2007] ECR I-1891., para. 20.

customs authorities<sup>15</sup>. In the hope of obtaining licences for at least 100 betting outlets in Italy, Stanley investigated the possibility of taking part in the tendering procedures, but realised that it could not meet the conditions concerning the transparency of share ownership because it formed part of a group quoted on the regulated markets. Accordingly, it did not participate in the tendering procedure and holds no licence for betting operations<sup>16</sup>.

Stanley operates in Italy through more than 200 agencies, commonly called 'data transmission centres' (DTCs). The DTCs supply their services in premises open to the public in which a data transmission link is placed at the disposal of bettors so that they can access the server of Stanley's host computer in the United Kingdom. In this way, bettors are able – electronically – to forward sports bets proposals to Stanley (chosen from lists of events, and the odds on them, supplied by Stanley), to receive notice that their proposals have been accepted, to pay their stakes and, where appropriate, to receive their winnings<sup>17</sup>. The DTCs are run by independent operators who have contractual links to Stanley. Mr Placanica, Mr Palazzese and Mr Sorricchio, the defendants in the main proceedings, are all DTC operators linked to Stanley<sup>18</sup>. According to the case-file forwarded by the Tribunale (District Court) di Teramo (Italy), Mr Palazzese and Mr Sorricchio applied, before commencing their activities, to Atri Police Headquarters for police authorisation in accordance with Article 88 of the Royal Decree. Those applications met with no response<sup>19</sup>.

The European Court of Justice examined very carefully the administrative and criminal aspects of the national legislation. The European Court of Justice stated that national legislation which prohibits the pursuit of the activities of collect-

---

15. Joined cases C-338/04, C-359/04 and C-360/04 *Criminal proceedings against Massimiliano Placanica (C-338/04), Christian Palazzese (C-359/04) and Angelo Sorricchio (C-360/04)* [2007] ECR I-1891., para. 21.

16. Joined cases C-338/04, C-359/04 and C-360/04 *Criminal proceedings against Massimiliano Placanica (C-338/04), Christian Palazzese (C-359/04) and Angelo Sorricchio (C-360/04)* [2007] ECR I-1891., para. 22.

17. Joined cases C-338/04, C-359/04 and C-360/04 *Criminal proceedings against Massimiliano Placanica (C-338/04), Christian Palazzese (C-359/04) and Angelo Sorricchio (C-360/04)* [2007] ECR I-1891., para. 23.

18. Joined cases C-338/04, C-359/04 and C-360/04 *Criminal proceedings against Massimiliano Placanica (C-338/04), Christian Palazzese (C-359/04) and Angelo Sorricchio (C-360/04)* [2007] ECR I-1891., para. 24.

19. Joined cases C-338/04, C-359/04 and C-360/04 *Criminal proceedings against Massimiliano Placanica (C-338/04), Christian Palazzese (C-359/04) and Angelo Sorricchio (C-360/04)* [2007] ECR I-1891., para. 25.

ing, taking, booking and forwarding offers of bets, in particular bets on sporting events, without a licence or a police authorisation issued by the Member State concerned, constitutes a restriction on the freedom of establishment and on the freedom to provide services, provided for in Articles 43 EC and 49 EC respectively. The objective of combating criminality by making the operators active in the sector subject to control as well as channelling the activities of betting and gaming into the systems controlled is capable of justifying those obstacles, a licensing system being capable, in that regard, of constituting an efficient mechanism. However, it is for the national courts to determine whether, in limiting the number of operators active in the betting and gaming sector, national legislation can genuinely contribute to that objective. By the same token, it will be for the national courts to ascertain whether those restrictions are suitable for achieving the objective pursued, do not go beyond what is necessary in order to achieve those objectives, and are applied without discrimination<sup>20</sup>.

Moreover, the ECJ stated that Articles 43 EC and 49 EC must be interpreted as precluding national legislation which excludes from the betting and gaming sector operators in the form of companies whose shares are quoted on the regulated markets. Independently of the question whether the exclusion of companies quoted on the regulated markets applies, in fact, in the same way to operators established in the Member State concerned and to those from other Member States, that blanket exclusion goes beyond what is necessary in order to achieve the objective of preventing operators active in the betting and gaming sector from being involved in criminal or fraudulent activities<sup>21</sup>. Articles 43 EC and 49 EC must be interpreted as precluding national legislation which imposes a criminal penalty on persons for pursuing the organised activity of collecting bets without a licence or a police authorisation as required under the national legislation, where those persons were unable to obtain licences or authorisations because that Member State, in breach of Community law, refused to grant licences or authorisations to them. Although in principle criminal legislation is a matter for which the Member States are responsible, Community law sets certain limits to their power, and such legislation may not restrict the fundamental freedoms guaranteed by Community law. Furthermore, a Member State may not apply a criminal penalty for failure to complete an administrative formality where such completion has been

---

20. Joined cases C-338/04, C-359/04 and C-360/04 *Criminal proceedings against Massimiliano Placanica (C-338/04), Christian Palazzese (C-359/04) and Angelo Sorricchio (C-360/04)* [2007] ECR I-1891, paras 49, 52, 57-58

21. Joined cases C-338/04, C-359/04 and C-360/04 *Criminal proceedings against Massimiliano Placanica (C-338/04), Christian Palazzese (C-359/04) and Angelo Sorricchio (C-360/04)* [2007] ECR I-1891, see paras 62, 64.

refused or rendered impossible by the Member State concerned in breach of Community law<sup>22</sup>.

Case C-42/07 *Liga Portuguesa*<sup>23</sup> is a very important ruling of the European Court of Justice, which was connected to online gambling. The European Court of Justice stated that Article 49 EC does not preclude legislation of a Member State which prohibits private operators established in other Member States, in which they lawfully provide similar services, from offering games of chance via the internet within the territory of that Member State. Admittedly, such legislation gives rise to a restriction of the freedom to provide services enshrined in Article 49 EC, by also imposing a restriction on the freedom of the residents of the Member State concerned to enjoy, via the internet, services which are offered in other Member States.

However, in the light of specific features associated with the provision of games of chance via the internet, the restriction at issue may be regarded as justified by the objective of combating fraud and crime. The grant of exclusive rights to operate games of chance via the internet to a single operator which is subject to strict control by the public authorities may confine the operation of gambling within controlled channels and be regarded as appropriate for the purpose of protecting consumers against fraud on the part of operators. As to whether the system in dispute is necessary, the sector involving games of chance offered via the internet has not been the subject of Community harmonisation.

A Member State is therefore entitled to take the view that the mere fact that a private operator lawfully offers services in that sector via the internet in another Member State, in which it is established and where it is in principle already subject to statutory conditions and controls on the part of the competent authorities in that State, cannot be regarded as amounting to a sufficient assurance that national consumers will be protected against the risks of fraud and crime, in the light of the difficulties liable to be encountered in such a context by the authorities of the Member State of establishment in assessing the professional qualities and integrity of operators. In addition, because of the lack of direct contact between consumer and operator, games of chance accessible via the internet involve different and more substantial risks of fraud by operators against consumers compared with the traditional markets for such games. Moreover, one can-

---

22. Joined cases C-338/04, C-359/04 and C-360/04 *Criminal proceedings against Massimiliano Placanica (C-338/04), Christian Palazzese (C-359/04) and Angelo Sorricchio (C-360/04)* [2007] ECR I-1891, see paras 68-69, 71.

23. Case C-42/07 *Liga Portuguesa de Futebol Profissional and Bwin International Ltd v Departamento de Jogos da Santa Casa da Misericórdia de Lisboa* [2009] ECR I-07633.

not rule out the possibility that an operator which sponsors some of the sporting competitions for which it accepts bets and some of the teams taking part in those competitions may be in a position to influence their outcome directly or indirectly, and, thus, increase its profits<sup>24</sup>.

Another case related with the offer of games of chance via the internet was Case C203/08 *Sporting Exchange*<sup>25</sup>. This case has to do with the Dutch legislation on gaming reserving a license to a single operator and with its compatibility with the freedom to provide services. After a careful analysis of the Dutch legislation and its previous case law on online gambling (especially Case C-42/07 *Liga Portuguesa*), the European Court of Justice stated that Article 49 EC must be interpreted as not precluding legislation of a Member State, such as the legislation at issue in the main proceedings, under which exclusive rights to organise and promote games of chance are conferred on a single operator, and which prohibits any other operator, including an operator established in another Member State, from offering via the internet services within the scope of that regime in the territory of the first Member State. Additionally, Article 49 EC must be interpreted as meaning that the principle of equal treatment and the consequent obligation of transparency are applicable to procedures for granting a licence to a single operator or for the renewal thereof in the field of games of chance, in so far as the operator in question is not a public operator whose management is subject to direct State supervision or a private operator whose activities are subject to strict control by the public authorities<sup>26</sup>.

In Case C-258/08 *Ladbrokes*<sup>27</sup>, the European Court of Justice discussed the compatibility with the freedom to provide services which are offered in the games of chance via the internet and with the freedom that the national legislation enjoy to reserve a license to a single operator. The European Court of Justice stated that national legislation, such as that at issue in the main proceedings, which seeks to curb addiction to games of chance and to combat fraud, and which in fact contributes to the achievement of those objectives, can be regarded as limiting betting activities in a consistent and systematic manner even where the holder(s) of an exclusive licence are entitled to make what they are offering on the market attracted by introducing new games and by means of advertising. It is for

---

24. Case C-42/07 *Liga Portuguesa de Futebol Profissional and Bwin International Ltd v Departamento de Jogos da Santa Casa da Misericórdia de Lisboa* [2009] ECR I-07633, paras 53-54, 67-73.

25. Case C-203/08 *Sporting Exchange Ltd v Minister van Justitie* [2010] ECR not reported yet (nry).

26. Case C-203/08 *Sporting Exchange Ltd v Minister van Justitie* [2010] ECR not reported yet.

27. Case C-258/08 *Ladbrokes Betting & Gaming Ltd and Ladbrokes International Ltd v Stichting de Nationale Sporttotalisator* [2010] ECR nry.

the national court to determine whether unlawful gaming activities constitute a problem in the Member State concerned, which might be solved by the expansion of authorised and regulated activities, and whether that expansion is on such a scale as to make it impossible to reconcile with the objective of curbing such addiction<sup>28</sup>. For the purpose of applying legislation of a Member State on games of chance which is compatible with Article 49 EC, the national courts are not required to determine, in each case, whether the implementing measure intended to ensure compliance with that legislation is suitable for achieving the objective of that legislation and is compatible with the principle of proportionality, in so far as that measure is necessary to ensure the effectiveness of that legislation and does not include any additional restriction over and above that which arises from the legislation itself.

Whether that implementing measure was adopted as a result of action by the public authorities to ensure compliance with national legislation or was applied by an individual in the context of a civil action to protect his rights under that legislation has no bearing on the outcome of the dispute before the national court<sup>29</sup>. Article 49 EC must be interpreted as not precluding legislation of a Member State, such as the legislation at issue in the main proceedings, under which exclusive rights to organise and promote games of chance are conferred on a single operator, and which prohibits any other operator, including an operator established in another Member State, from offering via the internet services within the scope of that regime in the territory of the first Member State<sup>30</sup>.

The next reference for a preliminary ruling received by the European Court of Justice dealt with the advertising of gambling activities. In Joined cases C-447/08 and C-448/08 *Sjöberg and Gerdin*<sup>31</sup>, the European Court of Justice declared that Article 49 EC must be interpreted as not precluding legislation of a Member State, such as that at issue in the main actions, which prohibits the advertising to residents of that State of gambling organised for the purposes of profit by private operators in other Member States. Article 49 EC must be interpreted as precluding legislation of a Member State subjecting gambling to a system of exclusive rights, according to which the promotion of gambling organised in another Mem-

---

28. Case C-258/08 *Ladbrokes Betting & Gaming Ltd and Ladbrokes International Ltd v Stichting de Nationale Sporttotalisator* [2010] ECR nry, para. 38.

29. Case C-258/08 *Ladbrokes Betting & Gaming Ltd and Ladbrokes International Ltd v Stichting de Nationale Sporttotalisator* [2010] ECR nry, para. 50.

30. Case C-258/08 *Ladbrokes Betting & Gaming Ltd and Ladbrokes International Ltd v Stichting de Nationale Sporttotalisator* [2010] ECR nry, para. 58.

31. Joined cases C-447/08 and C-448/08 *Criminal proceedings against Otto Sjöberg (C-447/08) and Anders Gerdin (C-448/08)* [2010] ECR nry

ber State is subject to stricter penalties than the promotion of gambling operated on national territory without a licence. It is for the referring court to ascertain whether that is true of the national legislation at issue in its main actions.

In the next case brought before the European Court of Justice, the public and social interest objectives of the national legislation establishing a public monopoly were scrutinized (Joined Cases C-316/07, C-358/07, C-359/07, C-360/07, C-409/07 and C-410/07 *Markus Stoß*<sup>32</sup>). The European Court of Justice stated that, on a proper interpretation of Articles 43 EC and 49 EC, in order to justify a public monopoly on bets on sporting competitions and lotteries, such as those at issue in the cases in the main proceedings, with an objective of preventing incitement to squander money and combat addiction to gambling the national authorities concerned do not necessarily have to be able to produce a study establishing the proportionality of the said measure which is prior to the adoption of the latter<sup>33</sup>.

Furthermore, a Member State's choice to use such a monopoly rather than a system authorising the business of private operators which would be permitted to carry on their business in the context of a non-exclusive legislative framework is capable of satisfying the requirement of proportionality, in so far as, as regards the objective concerning a high level of consumer protection, the establishment of the said monopoly is accompanied by a legislative framework suitable for ensuring that the holder of the said monopoly will in fact be able to pursue, in a consistent and systematic manner, such an objective by means of a supply that is quantitatively measured and qualitatively planned by reference to the said objective and subject to strict control by the public authorities<sup>34</sup>. Additionally, the fact that the competent authorities of a Member State might be confronted with certain difficulties in ensuring compliance with such a monopoly by organisers of

---

32. Joined cases C-316/07, C-358/07, C-359/07, C-360/07, C-409/07 and C-410/07 *Markus Stoß* (C-316/07), *Avalon Service-Online-Dienste GmbH* (C-409/07) and *Olaf Amadeus Wilhelm Happel* (C-410/07) v *Wetteraukreis and Kulpa Automatenservice Asperg GmbH* (C-358/07), *SOBO Sport & Entertainment GmbH* (C-359/07) and *Andreas Kunert* (C-360/07) v *Land Baden-Württemberg* [2010] ECR nry.

33. Joined cases C-316/07, C-358/07, C-359/07, C-360/07, C-409/07 and C-410/07 *Markus Stoß* (C-316/07), *Avalon Service-Online-Dienste GmbH* (C-409/07) and *Olaf Amadeus Wilhelm Happel* (C-410/07) v *Wetteraukreis and Kulpa Automatenservice Asperg GmbH* (C-358/07), *SOBO Sport & Entertainment GmbH* (C-359/07) and *Andreas Kunert* (C-360/07) v *Land Baden-Württemberg* [2010] ECR nry, paras. 81, 107

34. Joined cases C-316/07, C-358/07, C-359/07, C-360/07, C-409/07 and C-410/07 *Markus Stoß* (C-316/07), *Avalon Service-Online-Dienste GmbH* (C-409/07) and *Olaf Amadeus Wilhelm Happel* (C-410/07) v *Wetteraukreis and Kulpa Automatenservice Asperg GmbH* (C-358/07), *SOBO Sport & Entertainment GmbH* (C-359/07) and *Andreas Kunert* (C-360/07) v *Land Baden-Württemberg* [2010] ECR nry, paras. 83, 107



games and bets established outside that Member State, who, via the internet and in breach of the said monopoly, conclude bets with persons within the territorial area of the said authorities, are not capable, as such, of affecting the potential conformity of such a monopoly with the said provisions of the Treaty<sup>35</sup>. Moreover, on a proper interpretation of Articles 43 EC and 49 EC, in the current state of European Union law, the fact that an operator holds, in the Member State in which it is established, an authorisation permitting it to offer games of chance does not prevent another Member State, while complying with the requirements of European Union law, from making such a provider offering such services to consumers in its territory subject to the holding of an authorisation issued by its own authorities<sup>36</sup>.

Another case analysing national laws which prohibited offering games of chance via the internet was Case C46/08 *Carmen Media Group*<sup>37</sup>. In this Case, the ECJ stated that on a proper interpretation of Article 49 EC, an operator wishing to offer via the internet bets on sporting competitions in a Member State other than the one in which it is established does not cease to fall within the scope of the said provision solely because that operator does not have an authorisation permitting it to offer such bets to persons within the territory of the Member State in which it is established, but holds only an authorisation to offer those services to persons located outside that territory<sup>38</sup>. On a proper interpretation of Article 49 EC, where a system of prior administrative authorisation is established in a Member State as regards the supply of certain types of gambling, such a system, which derogates from the freedom to provide services guaranteed by Article 49 EC, is capable of satisfying the requirements of the latter provision only if it is based on criteria which are objective, non-discriminatory and known in advance, in such a way as to circumscribe the exercise of the national authorities' discretion so that

---

35. Joined cases C-316/07, C-358/07, C-359/07, C-360/07, C-409/07 and C-410/07 *Markus Stoß* (C-316/07), *Avalon Service-Online-Dienste GmbH* (C-409/07) and *Olaf Amadeus Wilhelm Happel* (C-410/07) v *Wetteraukreis and Kulpa Automatenservice Asperg GmbH* (C-358/07), *SOBO Sport & Entertainment GmbH* (C-359/07) and *Andreas Kunert* (C-360/07) v *Land Baden-Württemberg* [2010] ECR nry, para 107.

36. Joined cases C-316/07, C-358/07, C-359/07, C-360/07, C-409/07 and C-410/07 *Markus Stoß* (C-316/07), *Avalon Service-Online-Dienste GmbH* (C-409/07) and *Olaf Amadeus Wilhelm Happel* (C-410/07) v *Wetteraukreis and Kulpa Automatenservice Asperg GmbH* (C-358/07), *SOBO Sport & Entertainment GmbH* (C-359/07) and *Andreas Kunert* (C-360/07) v *Land Baden-Württemberg* [2010] ECR nry, para 116.

37. Case C46/08 *Carmen Media Group Ltd v Land Schleswig-Holstein, Innenminister des Landes Schleswig-Holstein* [2010] ECR nry.

38. Case C46/08 *Carmen Media Group Ltd v Land Schleswig-Holstein, Innenminister des Landes Schleswig-Holstein* [2010] ECR nry, para. 52.

it is not used arbitrarily. Furthermore, any person affected by a restrictive measure based on such a derogation must have an effective judicial remedy available to them<sup>39</sup>. On a proper interpretation of Article 49 EC, national legislation prohibiting the organisation and intermediation of games of chance on the internet for the purposes of preventing the squandering of money and combating addiction to gambling as well as protecting young persons from it may, in principle, be regarded as suitable for pursuing such legitimate objectives, even if the offer of such games remains authorised through more traditional channels. The fact that such a prohibition is accompanied by a transitional measure such as that at issue in the main proceedings is not capable of depriving the said prohibition of its suitability<sup>40</sup>.

## 5. A few comments on case law

The European Court of Justice was very cautious when it examined the national rules on gambling. In most cases, the ECJ confirmed the right of Member States to preserve their legal regimes in the area of gambling. Although some national provisions were deemed to infringe the fundamental freedoms of the European Union, Member States could justify these infringements in accordance with mandatory requirements in the public interest. The ECJ proclaimed that Member States are enjoying wide discretion in the justification of these infringements of fundamental freedoms. It is obvious that this wide discretion allows Member States to implement easily their public, moral and social considerations into the gambling market. The fact that each Member State possess a wide discretion in pursuing its public and social policy in the area of gambling means that we could possibly have as many as 27 different legal regimes in the internal market. As a matter of fact, the gambling market is regulated by national legal regimes that are quite diverse. This legal diversity is rather negative for the internal market of the European Union, which envisages market integration in the area of gambling.

The competence shown by the Member States to decide their national policies in this part of the internal market remains untouched. The ECJ tried to construct a framework which would not allow national policies to infringe the application of fundamental freedoms. Member States will not be prohibited to adopt an exclusive rights model or a licensing model. Those regulatory policies should apply in a non-discriminatory way to nationals and non-national market participants and should respect Community rules in principle. If a national measure infringes the

---

39. Case C46/08 *Carmen Media Group Ltd v Land Schleswig-Holstein, Innenminister des Landes Schleswig-Holstein* [2010] ECR nry, para. 90.

40. Case C46/08 *Carmen Media Group Ltd v Land Schleswig-Holstein, Innenminister des Landes Schleswig-Holstein* [2010] ECR nry, para. 111.

fundamental freedoms, it could be justified on certain grounds. Even if a national provision could not be justified, this does not mean that the whole national regulatory policy should be eliminated; it is this specific unjustified provision which should be removed or be adjusted appropriately<sup>41</sup>. According to case law, those national policies should be systematic and consistent and should not pursue arbitrary objectives<sup>42</sup>. Moreover, these policy objectives have to meet two separate criteria: on the one hand, there are consumer protection and other social issues they should address and on the other hand, there is the protections against crime and fraud issue. National legislatures should also not forget to establish this causal link between those grounds underpinning the available justifications and the dangers (e.g. addiction, crime, fraud etc.) which exist in the area of gambling and sports betting.

Member States retain their regulatory autonomy in the field of gambling and this might create problems in cross-border gambling activities. Online gambling constitutes the most common exercise of these cross-border gambling activities. This paper will criticize the ECJ's approach which does not result in market integration. It will seek to draw some conclusions on the market-making effects of the ECJ's case law on online gambling.

## 6. Conclusion

It is true that the market of gambling and sports betting is not an integrated part of the internal market. Member States have managed to maintain their regulatory autonomy in this area of law and can impose their own legislative choices and national standards on the regulation of their national gambling and sports betting market. There is no secondary Community legislation which could harmonize some national standards or facilitate cross-border market access of market participants or impose certain safeguards on this cross-border business activities. It is easily understood that the case law of the ECJ plays pivotal role in the clarification of this 'degree of latitude' that Member States maintain in this area of the internal market and in striking the right balance between this national competence and the aims of the internal market and its integration (Art. 2,3,14 EC Treaty). The case law stressed that those national regulatory choices should respect the rights of market participants to establish themselves or to provide services on EU level.

---

41. A. Littler, 'Regulatory perspectives on the future of interactive gambling in the internal market' [2008] *ELRev.* 211, 220.

42. A. Littler, 'Regulatory perspectives on the future of interactive gambling in the internal market' [2008] *ELRev.* 211, 220.

# ACTA and copyright in EU: a love or hate relationship?

---

---

Maria Daphne Papadopoulos

---

---

## I. Short history of ACTA

The Anti-Counterfeiting Trade Agreement (ACTA) constitutes one of the most debated copyright issues in the last years. ACTA aims to change the international framework providing a model for effective combating global proliferation of commercial scale counterfeiting and piracy. The objective of the new plurilateral<sup>1</sup> treaty is to improve the global standards for the enforcement of intellectually property rights (IPRs) in the international sphere and to become the new international standard for intellectual property enforcement.

The idea of this Agreement started on June 2005, when it was introduced by the Japanese Prime Minister Koizumi at the meeting of Group of Eight (G8) in Scotland.<sup>2</sup> The proposal for an anti-counterfeiting treaty was officially presented at the Second Global Congress to Combat Counterfeiting & Piracy<sup>3</sup> in 2005 and it was included in the Lyon Declaration<sup>4</sup>, adopted by the participants, where further consideration of the “Japan’s proposal for a new international treaty” was

- 
1. A plurilateral agreement implies that member countries would be given the choice to agree to new rules on a voluntary basis. This contrasts with the multilateral agreement, where all members are party to the agreement (read more at: <[http://wiki.answers.com/Q/What\\_is\\_the\\_difference\\_between\\_Plurilateral\\_agreement\\_and\\_Multilateral\\_agreement#ixzz1HQDyX2rc](http://wiki.answers.com/Q/What_is_the_difference_between_Plurilateral_agreement_and_Multilateral_agreement#ixzz1HQDyX2rc)> /accessed 01.09.2011). Etymologically, plurilateral and multilateral are synonyms for an agreement among more than two parties. In some international organizations, however, plurilateral is used to distinguish an agreement made among only some members of the whole from the multilateral agreements among all members (read more at: what is a Plurilateral Agreement? | eHow.com <[http://www.ehow.com/facts\\_7633632\\_plurilateral-agreement.html#ixzz1HQEKsmZ0](http://www.ehow.com/facts_7633632_plurilateral-agreement.html#ixzz1HQEKsmZ0)> /accessed 01.09.2011).
  2. Japan proposes new IP Enforcement Treaty, IP Watch (15 November 2005) online at <<http://www.ip-watch.org/weblog/2005/11/15/japan-proposes-new-ip-enforcement-treaty>> /accessed 01.09.2011 and Yu, Peter K., Six Secret (and Now Open) Fears of ACTA (June 14, 2010). SMU Law Review, Vol. 64, 2011 online at <<http://ssrn.com/abstract=1624813>> //accessed 01.09.2011, p. 4.
  3. See more information at: <[http://ccapcongress.net/2\\_Lyon.htm](http://ccapcongress.net/2_Lyon.htm)> /accessed 01.09.2011.
  4. The Lyon Declaration, 19 November 2005, p. 4, online at <<http://ccapcongress.net/archives/Lyon/files/OutcomesStatement20051115.pdf>> /accessed 01.09.2011.

recommended. The issue was reintroduced by Japan in the following Third Global Congress (2007 in Geneva)<sup>5</sup> and it was once more suggested to “Explore the proposal by the Government of Japan to develop an international treaty on the manufacturing and distribution of counterfeit and pirated goods, as well as consumer education.”<sup>6</sup> The issue of a new anti-counterfeiting treaty was discussed again in the next meeting of the G8 in Russia in 2006, where they reaffirmed their “commitment to strengthening individual and collective efforts to combat piracy and counterfeiting, especially trade in pirated and counterfeit goods”<sup>7</sup>. But the G8 was not a suitable forum for furthering any discussion on this subject, since it did not have any norm-setting capability. On the contrary, suitable and competent for such a discussion would be the World Intellectual Property Organization (WIPO) or the World Trade Organizations (WTO) or even the World Customs Organization (WCO). Finally, neither of those Organizations became the hosting forum of ACTA and the text was developed outside of them. This fact was a point of criticism against ACTA but not completely justified. Since the conclusion of Trade-Related Aspects of Intellectual Property Rights (TRIPs) Agreement in 1994 (WTO) and the WIPO Treaties in 1996 (WIPO), the developed countries were demanding a higher level of protection of intellectual property rights (IPRs). These efforts were expressed in proposals for ‘in-depth discussion’ on enforcement issues made at the TRIPs Council by the European Community (2006)<sup>8</sup> (with formal support from Japan, Switzerland and the United States)<sup>9</sup>, by the United States (2007)<sup>10</sup> and Switzerland (2007)<sup>11</sup>. All those attempts met strong resistance by the less

---

5. See more information at <[http://ccapcongress.net/3\\_Geneva.htm](http://ccapcongress.net/3_Geneva.htm)> /accessed 01.09.2011.

6. Suggestions Extending from the Third Global Congress, Geneva, January 30 and 31, 2007 online at <[http://ccapcongress.net/archives/Geneva/Files/Congress%20Recommendations\\_Geneva%20Jan%202007.pdf](http://ccapcongress.net/archives/Geneva/Files/Congress%20Recommendations_Geneva%20Jan%202007.pdf)> /accessed 01.09.2011, p. 3.

7. Statement on Combating IPR Piracy and Counterfeiting, July 16, 2006 online at <<http://en.g8russia.ru/docs/15.html>>/accessed 01.09.2011.

8. TRIPS Council, Communication from the European Communities, Enforcing Intellectual Property Rights: Border Measures, IP/C/W/471 (June 9, 2006). See also two earlier proposals TRIPS Council, Communication from the European Communities, Enforcement of Intellectual Property Rights, IP/C/W/468 (March 10, 2006); TRIPS Council, Communication from the European Communities, *Enforcement of Intellectual Property Rights*, IP/C/W/448 (June 9, 2005).

9. TRIPS Council, Joint Communication from the European Communities, United States, Japan and Switzerland, Enforcement of Intellectual Property Rights, IP/C/W/485 (November 2, 2006).

10. TRIPS Council, Communication from the United States, Enforcement of Intellectual Property Rights (Part III of the TRIPS Agreement): Experiences of Border Enforcement, IP/C/W/488 (Jan. 30, 2007).

11. TRIPS Council, Communication from Switzerland, Enforcement of Intellectual Property Rights: Communication and Coordination as a Key to Effective Border Measures, IP/C/W/492 (May 31, 2007).

developed countries, in most of the cases based on procedural grounds. The real reason though was that the less developed countries already had a hard time with the IP standards and the obligations stemmed from TRIPs and did not want a higher level for protection for IPRs<sup>12</sup>. Similar obstacles faced the efforts of the developed countries to expand the intellectual property enforcement in WIPO. Although the longest-standing international institution dealing with intellectual property, WIPO, is supposed to be the core of the international intellectual property system, over the last years this has fallen into question<sup>13</sup>. The adoption of Development Agenda for WIPO and specially the Recommendation 45, which calls on WIPO "to approach intellectual property enforcement in the context of broader societal interests and especially development oriented concerns"<sup>14</sup>. and the establishment of the Advisory Committee on Enforcement (ACE)<sup>15</sup> were not enough and certainly not encouraging, since norm-setting was excluded explicitly from the Mandate of the ACE. No essential development was shown despite the efforts of some members to the contrary. The lack of any initiative and any progress in the field of IP enforcement forced developed countries to other fora and to other solutions, such as the conclusion of bilateral and –in the case of ACTA- of plurilateral agreements.

It was not until October 2007, when the first unofficial negotiations for ACTA took place<sup>16</sup>. The key negotiating parties were Japan, the United States and the European Union. The other negotiating Parties included Canada, Mexico, New Zealand, South Korea, and Switzerland<sup>17</sup>. Australia, Morocco, Singapore and the 27 members of the European Union joined later the negotiations<sup>18</sup>. The negotia-

---

12. See analytically Yu, p. 10f.

13. ACTA was not the only threat to the leadership of WIPO in the world IP system. The Universal Copyright Convention was established under UNESCO in 1952 and TRIPs under WTO in 1994, Bannerman, Sara. 2010. WIPO and the ACTA Threat. PIJIP Research Paper no. 4. American University Washington College of Law, Washington, DC (January 9, 2010) online at <<http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1004&context=research>>/accessed 01.09.2011.

14. WIPO, The 45 Adopted Recommendations Under the WIPO Development Agenda online at <<http://www.wipo.int/ip-development/en/agenda/recommendations.html>> /accessed 01.09.2011.

15. Information about the WIPO Advisory Committee on Enforcement online at <<http://www.wipo.int/enforcement/en/ace/>> /accessed 01.09.2011 .

16. The first official round of negotiation took place in June 2008 in Geneva (border measures) online at <[http://trade.ec.europa.eu/doclib/docs/2008/june/tradoc\\_139085.pdf](http://trade.ec.europa.eu/doclib/docs/2008/june/tradoc_139085.pdf)> /accessed 01.09.2011.

17. The United Arab Emirates participated in the first round of negotiations but it had not attended the subsequent rounds of negotiations.

18. Ch. 6, Article 39, n. 17, p. 23 ACTA (text of 3.12.2010).

tions ended on October 2010 after 11 rounds<sup>19</sup>. The final text of ACTA includes six chapters. The Initial Provisions (Chapter I), where the parties describe the nature and scope of the agreement and its relationship to domestic laws and it includes definitions of terms used in the agreement. In the second chapter, legal framework for enforcement of intellectual property rights, the parties agree to provide various legal means to enforce IPRs (civil enforcement provisions dealing with issues such as damages, injunctions to stop further infringements, recovery of costs and attorneys' fees, and destruction of infringing goods, border measures, criminal enforcement, enforcement of intellectual property rights in the digital environment). In chapter III, enforcement practices, Parties agree to promote practices that contribute to effective enforcement of IPRs, such as specialization, data collection and analysis, internal coordination, and stakeholder consultation. Chapter IV, international cooperation, provides that the parties agree to cooperate to realize effective protection of IPRs. In chapter V, institutional Arrangements, a committee is established not only to review the operation of the agreement but to serve as a forum to discuss enforcement issues, as well as to handle any matter relating to the agreement. In the last chapter, Final Provisions, the parties agree on matters concerning the signature and entry into force of the Agreement and on other technical matters<sup>20</sup>.

19. Round 1: Geneva, Switzerland (June 2008) (border measures), Round 2: Washington, USA (July 2008) (border measures and civil enforcement of intellectual property rights, <[http://trade.ec.europa.eu/doclib/docs/2008/august/tradoc\\_140017.pdf](http://trade.ec.europa.eu/doclib/docs/2008/august/tradoc_140017.pdf)> /accessed 01.09.2011), Round 3: Tokyo, Japan (October 2008) (civil and criminal enforcement of intellectual property rights, <[http://trade.ec.europa.eu/doclib/docs/2008/october/tradoc\\_141203.pdf](http://trade.ec.europa.eu/doclib/docs/2008/october/tradoc_141203.pdf)> /accessed 01.09.2011), Round 4: Paris, France (December 2008) (criminal enforcement, international cooperation, enforcement practices, institutional arrangements, and internet distribution and information technology, <[http://trade.ec.europa.eu/doclib/docs/2009/january/tradoc\\_142118.pdf](http://trade.ec.europa.eu/doclib/docs/2009/january/tradoc_142118.pdf)> /accessed 01.09.2011), Round 5: Rabat, Morocco (July 2009) (international cooperation, enforcement practices, institutional arrangements, and transparency matters, <<http://trade.ec.europa.eu/doclib/html/144136.htm>> /accessed 01.09.2011), Round 6: Seoul, South Korea (November 2009) (enforcement of rights in the digital environment, criminal enforcement, and transparency matters, <[http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc\\_145302.pdf](http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc_145302.pdf)> /accessed 01.09.2011), Round 7: Guadalajara, Mexico (January 2010) (civil enforcement, border enforcement and enforcement of rights in the digital environment), Round 8: Wellington, New Zealand (April 2010) (civil enforcement, border measures, criminal enforcement and special measures for the digital environment), Round 9: Lucerne, Switzerland (<[http://trade.ec.europa.eu/doclib/docs/2010/july/tradoc\\_146292.pdf](http://trade.ec.europa.eu/doclib/docs/2010/july/tradoc_146292.pdf)> /accessed 01.09.2011) (June 2010), Round 10: Washington, D.C., USA, August 2010 and Round 11: Tokyo, Japan (October, 2010), <<http://ec.europa.eu/trade/creating-opportunities/trade-topics/intellectual-property/anti-counterfeiting/>> /accessed 01.09.2011).

20. ACTA fact sheet and guide to public draft text, Office of the United States Trade Representative online at <<http://www.ustr.gov/about-us/press-office/fact-sheets/2010/acta>>

Another concern regarding ACTA was the lack of formal transparency in the negotiations process<sup>21</sup>. The first available draft of ACTA has leaked on January 2010<sup>22</sup>, while the first official draft of ACTA was not released until April 2010.<sup>23</sup> Some other drafts of ACTA were leaked afterwards<sup>24</sup>. A consolidated draft was released in October 2010<sup>25</sup> and the nearly identical draft was released on December 3, 2010<sup>26</sup>. The Commission published on May 2011 a new version of ACTA<sup>27</sup>, while the official text has been published on August 23, 2011, with Document 12196/11<sup>28</sup>. The lack of transparency and the secrecy of ACTA negotiations was heavily criticized by the European Parliament, NGOs and other civil liberties groups. The European Parliament reacted in this respect issuing two contradic-

---

fact-sheet-and-guide-public-draft-text> /accessed 01.09.2011.

21. See analytically, Geist, Michael, ACTA Guide Part III: Transparency and ACTA secrecy online at <<http://www.mp3newswire.net/stories/0102/ACTA-guide-3.htm>> /accessed 01.09.2011.
22. ACTA Draft – January 18, 2010 online at <[http://euwiki.org/ACTA/Informal\\_Predecisional\\_Deliberative\\_Draft\\_18\\_January\\_2010](http://euwiki.org/ACTA/Informal_Predecisional_Deliberative_Draft_18_January_2010)> /accessed 01.09.2011.
23. Official Consolidated Text – April 21, 2010 online at [http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc\\_146029.pdf](http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf) /accessed 01.09.2011.
24. ACTA July 2010 draft online at <<http://www.laquadrature.net/en/new-acta-leak-2010-07-13-consolidated-text-luzern-round>> /accessed 01.09.2011 and the draft of August 2010 online at <[http://keionline.org/sites/default/files/acta\\_aug25\\_dc.pdf](http://keionline.org/sites/default/files/acta_aug25_dc.pdf)> /accessed 01.09.2011.
25. Consolidated Draft of October 2, 2010 online at <[http://trade.ec.europa.eu/doclib/docs/2010/october/tradoc\\_146699.pdf](http://trade.ec.europa.eu/doclib/docs/2010/october/tradoc_146699.pdf)> /accessed 01.09.2011. In November a finalized text of the Treaty subject to legal review was released online at <[http://trade.ec.europa.eu/doclib/docs/2010/november/tradoc\\_147002.pdf](http://trade.ec.europa.eu/doclib/docs/2010/november/tradoc_147002.pdf)> /accessed 01.09.2011.
26. Online at <[http://trade.ec.europa.eu/doclib/docs/2010/december/tradoc\\_147079.pdf](http://trade.ec.europa.eu/doclib/docs/2010/december/tradoc_147079.pdf)> /accessed 01.09.2011. Following legal verification of the final text, the proposed agreement will then be ready to be submitted to the parties' competent authorities to undertake the relevant domestic processes.
27. Online at <[http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc\\_147937.pdf](http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf)> /accessed 01.09.2011. The text included minor changes. It was removed: "3 December 2010 (the date the prior "final" text was made) and it was changed: "This Agreement shall remain open for signature by participants in its negotiation,17 and by any other WTO Members the participants may agree to by consensus, from 31 March 2011 until 31 March 2013" to: "This Agreement shall remain open for signature by participants in its negotiation,17 and by any other WTO Members the participants may agree to by consensus, from 1 May 2011 until 1 May 2013".
28. Online at <<http://register.consilium.europa.eu/pdf/en/11/st12/st12196.en11.pdf>> /accessed 01.09.2011.



tory resolutions: one on March 10, 2010<sup>29</sup> and a second one on November 24, 2010<sup>30</sup>. In the first resolution the European Parliament not only expressed “its concern over the lack of transparent progress in the conduct of the ACTA negotiations” but clearly threatened “to take suitable action, including bringing a case before the Court of Justice” against the Commission, which was negotiating on behalf of the EU, if it did not share more information about all stages of the negotiations. On the contrary, in November 2010, the European Parliament welcomed the controversial intellectual property treaty as “a step in the right direction”.

The decision of the European Ombudsman<sup>31</sup> justified the fact that ACTA had been negotiated as a trade agreement and not as an enforcement treaty. The disclosure of the documents would be “detrimental to the international relations between EU and those (negotiating) countries”, “it would be prejudicial to the EU’s interest in the conduct of the negotiations” and “would have a negative effect on the climate of confidence in the ongoing negotiations, and that open and constructive cooperation might be hampered.” This secretive approach increased the possibilities for a more successful negotiation, shielded from external influence and pressure, i.e. political implications from the capitals and oppositions from civil society groups.

Notwithstanding those implications by releasing ACTA documents, still the other side supports that ACTA is not *per se* a trade agreement<sup>32</sup> that would justify such

29. European Parliament Resolution of 10 March 2010 on the transparency and state of play of the ACTA negotiations online at <<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0058+0+DOC+XML+V0//EN>>/accessed 01.09.2011.

30. European Parliament Resolution of 24 November 2010 on the ACTA online at <<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0432+0+DOC+XML+V0//EN>>/accessed 01.09.2011.

31. European Ombudsman’s decision on complaint 90/2009/(JD)OV (23.07.2010) relating to denied access to ACTA documents online at <http://people.ffii.org/~ante/acta/ombudsman-2010-7-23.pdf> /accessed 01.09.2011. Relevant is also an informal agreement among ACTA parties, the ‘Maintaining Confidentiality of Documents’, expressing the understanding that intergovernmental negotiations dealing with issues that have an economic impact may not necessarily take place in public and that negotiations are bound by a certain level of discretion online at <<http://www.google.com/url?sa=t&source=web&cd=1&ved=OCBgQFjAA&url=http%3A%2F%2Fwww.wcl.american.edu%2Fpijip%2Fdownload.cfm%3Fdownloadfile%3D7FC54F05-A112-5891-1CA6A91F7563BF11%26typename%3DdmFile%26fieldname%3Dfilename&ei=yy-UTeX3I4aChQei1oDwCA&usq=AFQjCNFC7X1i7cXxjlhK497SnAbVZ5yWtA>>/accessed 01.09.2011.

32. ACTA does not intend to facilitate or promote trade, it does not set preconditions for trade and it does not remove barriers to trade and therefore, the claims to be a trade agreement are weak, unless we adopt a very broad conception of ‘trade agreements’. See analytically

a degree of secrecy but it focuses primarily on intellectual property enforcement and this does not deserve the same type of protection as a trade agreement, despite the opposite official position of the European Commission<sup>33</sup>.

In any case it has to be admitted that even in a later stage, transparency made its entry during the ACTA negotiations, since in one way or another several drafts of the agreement were given out before its finalization and there were some spectacular changes in certain points that gathered the most negative comments. Those changes came mainly due to the negotiations of the parties but, also till to a certain point due to the pressure of the different civil society organizations. Besides, total transparency from the beginning of the negotiations would not be so helpful, since it is common at early stages of a Treaty's negotiation not to have a text but a pile of proposals, that need a great deal of elaboration before starting to form a consolidated text.

Apart from the lack of transparency, another major issue in the European Union was whether the provisions of ACTA are in line with the current EU IPRs regime and compatible with the relevant *acquis communautaire*. This is also the subject of the present paper. The official position of the European Commission and of the European Parliament<sup>34</sup> is that ACTA is in line with current EU regime or even less demanding and therefore the agreement is already fully implemented by the cur-

---

Weatherall, Politics, Compromise, Text and the failures of the Anti-Counterfeiting Trade Agreement, *Sydney Law Review* Vol. 33, p. 233.

33. Yu, p. 22-23. See the answer that was given by Mr De Gucht on behalf of the Commission (21.1.2011) E-8847/2010 online at <<http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-8847&language=EL>>/accessed 01.09.2011: "Regarding the first question about whether ACTA qualifies as a trade agreement, the issue that needs to be settled is under which competences the Union can potentially ratify the Agreement. It is clear that the EU's competence under the common commercial policy (Article 207 TFEU), which includes 'the commercial aspects of intellectual property', provides an EU competence for the matters regulated in ACTA. In this sense, therefore, ACTA can be considered a 'trade' agreement. ... As regards transparency, trade agreements, based on Article 207 TFEU, are subject to the same rules on transparency as applicable to other negotiations, but Article 207 requires that the Parliament be kept fully informed. International negotiations are always subject to a certain degree of confidentiality because the parties need a minimum level of confidentiality to feel comfortable enough to make concessions or to try different options".

34. European Parliament Resolution of 24 November 2010 on the Anti-Counterfeiting Trade Agreement (ACTA) online at <<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0432+0+DOC+XML+V0//EN>>/accessed 01.09.2011.

rent EU legislation, and it fully respects fundamental rights, freedoms and civil liberties, such as the protection of personal data<sup>35</sup>.

According to the Commission ACTA is about enforcement of existing law and not about substantive law. *L' acquis Communautaire* is about substantive law and this is why it remains unchanged. Additionally, ACTA builds mainly upon the main international standards, which are set by TRIPs. ACTA takes TRIPs agreement as a common ground, defines additional obligations of its contracting parties<sup>36</sup> and provide enforcement tools where TRIPs are considered to fall short<sup>37</sup>.

Nevertheless, a group of prominent law professors seem to refute European's Commission claim that ACTA is compatible with existing European legal framework. The signatories of the 'Opinion of European Academics on the Anti-counterfeiting Trade Agreement' (20.01.2011)<sup>38</sup> assert that: "Contrary to the European Commission's repeated statements and the European Parliament's resolution of 24 November 2010, certain ACTA provisions are not entirely compatible with EU law and will directly or indirectly require additional action on the EU level".

A few months afterwards in april 2010 the European Commission's Directorate-General for Trade has released a working paper that responds to this widely cited Opinion Document. The Commission in its point-by-point rebuttal holds that even though ACTA is not entirely consistent with existing EU law, the compatibility of ACTA with the *acquis communautaire* is not problematic.

Additionally, another study commissioned by the European Parliament Committee on international trade was conducted by the Directorate-General for external

35. See answers given by Mr De Gucht on behalf of the Commission at parliamentary questions online at <<http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-8847&language=EL>>, <<http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2010-9179&language=EN>> and the Debate on ACTA on 20 October 2010 online at <<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20101020+ITEM-016+DOC+XML+V0//EN>>/all accessed 01.09.2011.

36. Article 1 par. 1 ACTA. Metzger Axel, A Primer on ACTA: what Europeans Should Fear about the Anti-Counterfeiting Trade Agreement, 1 (2010) JIPITEC 109, par. 5.

37. Shayerah Ilias, The Proposed Anti-Counterfeiting Trade Agreement: Background and key issues, CRS Report for Congress, March 12, 2010, p. 1. See analytically the provisions of ACTA that provide value compared to existing international standards and in particular TRIPs at EUROPEAN COMMISSION Directorate-General for Trade, 3 November 2010 "LIMITED" NOTE FOR THE ATTENTION OF THE INTA COMMITTEE, ANNEX 1 online at <[http://www.laquadrature.net/wiki/ACTA\\_EC\\_WTO\\_TRIPS\\_20101109](http://www.laquadrature.net/wiki/ACTA_EC_WTO_TRIPS_20101109)>/accessed 01.09.2011.

38. Online at <[http://www.iri.uni-hannover.de/tl\\_files/pdf/ACTA\\_opinion\\_110211\\_DH2.pdf](http://www.iri.uni-hannover.de/tl_files/pdf/ACTA_opinion_110211_DH2.pdf)>/accessed 01.09.2011.

policies of the Union<sup>39</sup>. The study addresses two key questions regarding ACTA: whether it is in conformity with the EU *acquis* and with the existing international obligations of the EU and its member states.

Finally, what is the case? Is the new anti-counterfeiting agreement a step forward to combating effectively counterfeiting and piracy, enhancing the legal framework by establishing 'a new standard of IP enforcement' and improving international cooperation in IPR enforcement, fully in line with the European *acquis* or is it a new instrument that conflicts with civil liberties and legitimate economic concerns not based on IPRs, blemished by the murky negotiation history of ACTA in many aspects not in conformity with the European IP standards and that's why not to be ratified by the Council and the European Parliament? And coming to the title of the paper: ACTA and copyright in EU: Is a love or a hate relationship?

In order to answer this question we will go through the chapters of ACTA and we will examine them carefully.

## II. Comments on the ACTA Chapters

### 1. Definitions

In ACTA "pirated counterfeited goods means any goods which are copies made without the consent of the rightholder or person duly authorized by the right-holder in the country of production and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under the law of the country in which the procedures set forth in Chapter II (Legal Framework for Enforcement of Intellectual Property Rights) are invoked"<sup>40</sup>.

ACTA's references to 'pirated copyright goods' though could be misleading and not politically correct. The use of the term 'piracy' as a synonym for copyright infringement is not only technically incorrect but also highly prejudicial creating a false equivalence between the violation of an economic right and a dangerous crime involving physical violence. Therefore, the term 'piracy' should have been

---

39. The Anti-Counterfeiting Trade Agreement (ACTA): An Assessment, European Parliament – Directorate-General for External Policies/Policy Department online at <<http://www.laquadrature.net/files/INTA%20-%20ACTA%20assessment.pdf>>/accessed 01.09.2011, p. 51.

40. ACTA, Article 5. In TRIPs 'pirated copyright goods' were defined as infringing "under the law of the country of importation", Article 51 ("pirated copyright goods' shall mean any goods which are copies made without the consent of the rightholder or person duly authorized by the rightholder in the country of production and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under the law of the country of importation").

replaced with the more appropriate term of 'copyright infringement'<sup>41</sup>. In European directives 'piracy' is never used in the context of 'copyright infringement'.

Both in TRIPS and in ACTA the language is awkward concerning cases where goods are put on the market lawfully but without the permission of the right owner, such as in the case of a compulsory license or an exception to rights. The TRIPS definitions, in the context of suspension of release by customs authorities, refer specifically to the border measures, while the ACTA definitions are more general<sup>42</sup>.

The European Commission pushed for some last changes, as it was concerned that the original definition would create obligations to destroy goods that were not infringing rights in EU. Exceptions and limitations, such as private copy rules in national rules could disallow procedures from jurisdictions where no such limitations exist<sup>43</sup>.

Another important point worth to be mentioned in this Section of General Definitions is the notion of 'person'. According to ACTA (Article 5) 'person' means a natural or a legal person. This definition heighten liability for companies accused as direct infringers, such as search engines and give the possibility to the rightholders to go after them for direct infringement. And for the purposes of ACTA 'rightholders' include also "*a federation or an association having the legal standing to assert rights in intellectual property*" and not only the ones that created the infringed good<sup>44</sup>.

Nothing in this general definitions section though seems to be contrary to the European *acquis*.

## 2. Civil enforcement

### Injunctions

After an article that contains some general rules on civil procedures (Article 7 ACTA) - similar to Article 3 of Directive 2004/48<sup>45</sup> (hereinafter the Enforcement

41. Concerns with April 2010 ACTA Text (23.04.2010) online at <<http://www.librarycopyrightalliance.org/bm~doc/consolidatedtextcomments423.pdf>>/accessed 01.09.2011.

42. KEI, The October 2, 2010 version of the ACTA text online at <<http://keionline.org/node/962>>/accessed 01.09.2011.

43. Ermert, 'Final final' ACTA Text Published; More Discussion Ahead For EU online at <<http://www.ip-watch.org/weblog/2010/12/06/%E2%80%98final-final%E2%80%99-acta-text-published-more-discussion-ahead-for-eu>> /accessed 01.09.2011. See also regarding the definition of 'pirated copyright goods' later in the section Other remedies.

44. Kaminski, Margot, 2011. An overview and the Evolution of the Anti-Counterfeiting Trade Agreement, PIJIP Research Paper no. 19. American University Washington College of law, Washington, DC, p. 10.

45. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, OJ L 157, 20.04.2004, p. 45-86.

Directive) - the first civil remedy of ACTA concerns injunctions. According to article 8 par. 1 ACTA "Each Party shall provide that, in civil judicial proceedings concerning the enforcement of intellectual property rights, its judicial authorities have the authority<sup>46</sup> to issue an order against a party to desist from an infringement, and inter alia, an order to that party or, where appropriate, to a third party over whom the relevant judicial authority exercises jurisdiction, to prevent goods that involve the infringement of an intellectual property right from entering into the channels of commerce." The wording presents similarities to the corresponding Article 11 of the Enforcement Directive<sup>47</sup>. The difference is that ACTA adds 'inter alia' and consequently has a broader formulation of the third party including also third parties that are not intermediaries. This may impact access to ICT sector. Another difference is that in the Enforcement Directive exists also the possibility of article 12, which provides that under certain circumstances (in appropriate cases, if the infringer asks for it, if that person acted unintentionally and without negligence, if execution of the measures in question would cause him/her disproportionate harm and if pecuniary compensation to the injured party appears reasonably satisfactory) the competent judicial authorities may order pecuniary compensation instead of applying the injunction<sup>48</sup>. The possibility of applying pecuniary compensation as an alternative to injunction does not exist in ACTA explicitly. Nevertheless, there is also no prohibition to a party of ACTA to supply the judicial authorities with the authority to order pecuniary compensation as an alternative and consequently the pecuniary compensation option provided in the Enforcement Directive remains and it is fully in line with ACTA<sup>49</sup>. In any case it has to be noted that this option of article 12 of the Enforcement Directive is optional and that it can be applied only in exceptional cases. But most importantly

---

46. The function of the words 'have the authority' is to address the issue of judicial discretion not that of general availability (see Interpretation of Article 44 TRIPs online at <[http://www.wto.org/english/res\\_e/booksp\\_e/analytic\\_index\\_e/trips\\_03\\_e.htm#article44B](http://www.wto.org/english/res_e/booksp_e/analytic_index_e/trips_03_e.htm#article44B)>/accessed 01.09.2011).

47. "Member States shall ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement. Where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC".

48. Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 2. Similar possibility exists and in Article 44 par. 1 of TRIPs Agreement.

49. Commission Services Working Paper (Comments on the Opinion of European Academics on Anti-Counterfeiting Trade Agreement) online at <[http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc\\_147853.pdf](http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc_147853.pdf)> published in 27.04.2011 /accessed 01.09.2011, p. 6.

this possibility of Article 12 of the Enforcement Directive mirrors the general principle of proportionality, which is also respected in ACTA and it is applied to all enforcement measures according to article 6 par. 4 ACTA. Thus, it could be argued that Article 12 of the Enforcement Directive is in conformity with ACTA, serving the objective of preventing disproportionate consequences.<sup>50</sup> So, actually it is not true that this option would be lost or at least called in question, if article 8 par. 1 ACTA is enacted in this form, as the European Academics support<sup>51</sup>.

## Damages

In Article 9 par. 1 ACTA a set of criteria is recorded specifying the amount of compensatory damages in civil judicial proceedings concerning the enforcement of IPRs, after having stated in the very first paragraph the basic principle, i.e. that the damages shall be “adequate to compensate for the injury the rightholder has suffered as a result of the infringement”. The calculation of damages in civil IP cases is controversial, given the difficulty to estimate the value of the infringement. Rightholders find it challenging to prove that a decrease of their revenues is caused by the activities of the infringer<sup>52</sup>. ACTA encourages judges to consider “any legitimate measure of value the rightholder submits, which may include lost profits, the value of the infringed goods or services measured by the market price, or the suggested retail price”. Some of the above listed criteria (article 9 par. 1 ACTA) are provided for also in article 13 par. 1 of the Enforcement Directive, some other are not. It has been supported that “The value of the infringed goods or services measured by the market price, or the suggested retail price” does not reflect the economic loss suffered by the rightholder<sup>53</sup>. The Enforcement Directive uses damages appropriate to the actual prejudice suffered, including lost profits. The introduction of the possibility of using not only the market price but the suggested retail price as a measure of the value of the infringed good could bring more profit than the actual damage -according to the ACTA sceptics- given that the suggested retail price is higher than the actual prejudice. In practice, the effectiveness of this measurement is disputed<sup>54</sup>. In the case of a downloaded movie, this does not necessarily means that the downloader would consider al-

---

50. Ficsor, Compatibility of the Anti-Counterfeiting Trade Agreement (ACTA) with the EU legal system, Annual Conference on European Copyright Law, 19-20 May 2011, slide 29.

51. Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 2.

52. Metzger, p. 111.

53. Opinion of European Academics on the Anti-Counterfeiting Trade Agreement, p. 2.

54. Against the effectiveness see Opinion of European Academics on the Anti-Counterfeiting Trade Agreement, p. 2 and Kaminski, p. 12 and in favor see Commission Services Working Paper, p. 6-7 and Ficsor, slide 32. More specifically, Ficsor states that “the suggestion that that what the owners of rights may have obtained in the market as a counter-value of their

ternatively acquiring legally the dvd. So, the presumption that ACTA carries out, i.e. that the infringers' profits equal the amount of the damages claimed by the rightholder, is not always correct, since on the one hand the infringers do not sell infringing products to process similar to the legal ones and on the other hand sometimes they do not even sell<sup>55</sup>.

But in the case that this criterion is not so successful and accurate in calculating the injury suffered by the rightholders, the judge would not take it into account due to the 'may' language of the relevant sentence listing the possible criteria in a non-exhaustive manner. The criteria listed in article 9 of ACTA are not obligatory for the ACTA parties.

Additionally, in ACTA the infringement committed in good faith is not regulated and damages cannot be awarded for this kind of infringement, contrary to Article 13 par. 2<sup>56</sup> of the Enforcement Directive, according to which the mere existence of an infringement is a sufficient justification for the rightholder to claim damages. However, this case is also not mandatory for the national legislation, since the provision gives the possibility only -and not the obligation- to the member states to provide with this authority the courts and also to the courts the chance to award such damages.

Moreover, the opponents of ACTA claim that the compensatory damages (article 9 par. 1) and the infringer's profits (article 9 par. 2) may be ordered cumulatively, since there is no clarity regarding the alternative application of the different possibilities of article 9 par. 1 and 2 ACTA. In agreement to this view this cumulative application would not be in accordance with Article 13 of the Enforcement Directive and it would raise the amount of damages for copyright infringement<sup>57</sup>. On the contrary, the Commission supports that the formulation of ACTA does not mean that the amounts stipulated in the paragraphs of article 9 are cumulative and would result to an increase the level of applicable damages. As a supportive argument to their position, they invoke the last sentence of article 9 par. 2, which states that the infringer's profit may be presumed to be the amount of damages referred to article 9 par. 1, which seems to exclude the cumulative application<sup>58</sup>.

---

goods and services must not be taken into account among the factors to calculate damages is so much absurd that it is hardly necessary to state that it is completely unfounded."

55. Kaminski, p. 12.

56. "Where the infringer did not knowingly, or with reasonable grounds to know, engage in infringing activity, Member States may lay down that the judicial authorities may order the recovery of profits or the payment of damages, which may be pre-established".

57. Opinion of European Academics on the Anti-Counterfeiting Trade Agreement, p. 2.

58. Commission Services Working Paper, p. 7 and Ficsor, slide 33.



At this point it has to be mentioned that the infringer's profit is not unknown in the Enforcement Directive but it is included in the examples of the criteria that the judge should take into account, when he sets the damages (article 13 par. 1(a) of the Enforcement Directive). This could imply also the application of cumulative criteria, which in turn could bring an increase of the amount of the damages, in the same way that this could happen in ACTA parties, if we do accept this interpretation to the relevant ACTA provision. This possible increase of the amount of the damages would not be necessarily negative, since the aim is the damages to "*be adequate to compensate for the injury the rightholder has suffered*" (article 9 par. 1 ACTA but also article 45 par. 1 TRIPs) or "*to pay to the rightholder damages appropriate to the actual prejudice suffered*" (article 13 par. 1 of the Enforcement Directive). Besides, there is always the safeguard of the proportionality principle (foreseen also in ACTA as a general principle in article 6 par. 3) that would not allow any potential unproportionality in the case of cumulative application of criteria<sup>59</sup>. Finally, it has to be mentioned that in the recent report on the application of the Enforcement Directive, it has been stated that "*damage awards do not currently appear to effectively dissuade potential infringers from engaging in illegal activities. This is particularly so where damages awarded by the courts fail to match the level of profit made by the infringers*"<sup>60</sup>. This could imply that the award of damages model adopted in the Enforcement Directive is not so successful and it could be improved, maybe even with the small differences that ACTA introduces.

Consequently, after this analysis ACTA's provisions of damages seem not to be in conflict with the European *acquis communautaire*.

## Other remedies

As a corrective measure ACTA provides for destruction of pirated copyright goods at the rightholder's request. ACTA does not provide any choice of other corrective measures, such as recall and definitive removal from the channels of commerce, measures available in the Enforcement Directive (Article 10 par. 1)<sup>61</sup>. More spe-

---

59. Ficsor, slide 33.

60. Report from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, Application of Directive 2004/48/EC, COM(2010) 779 final, 22.12.2010 online at <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0779:FIN:EN:PDF>> /accessed 01.09.2011, p. 8.

61. "Without prejudice to any damages due to the rightholder by reason of the infringement, and without compensation of any sort, Member States shall ensure that the competent judicial authorities may order, at the request of the applicant, that appropriate measures be taken with regard to goods that they have found to be infringing an intellectual property right and, in appropriate cases, with regard to materials and implements principally used in the creation or manufacture of those goods. Such measures shall include:

cifically ACTA requires parties to give judicial authorities the authority to destroy civil infringing goods at the rightholder's request<sup>62</sup> and without any compensation at all "except in exceptional circumstances". ACTA adopts the alternative of the disposal outside the channels of commerce -parallel to the destruction- only for material and implements, the predominant use of which has been in manufacture or creation of such infringing goods without compensation and without any undue delay, possibility that exists also in the Enforcement Directive (Article 10 par. 1: "... in appropriate cases, with regard to materials and implements principally used in the creation or manufacture of those goods"). Still there are some concerns that although the destruction of infringing goods is envisaged by the Enforcement Directive as one of the remedies that can be invoked in addition to damages, the other two remedies (the recall and the definitive removal of the products from the channels of commerce) are not provided for. Nevertheless, nothing prevents EU empowering judicial authorities to apply other remedies, to the extent that these authorities are also empowered as to do so, as ACTA requires<sup>63</sup>.

Unlike the Enforcement Directive (Article 10 par. 3) and TRIPs (Article 46), ACTA does not contain clearly the requirement of the "proportionality between the seriousness of the infringement and the remedies ordered as well as the interest of third parties". Nonetheless, as it has been already stated, this provision appears to be reflected in the general obligations section (Section 1, Chapter II), in article 6 par. 3 ACTA, where it is provided that "in implementing the provisions of this Chapter, each Party shall take into account the need for proportionality between the seriousness of the infringement, the interests of third parties and the applicable measures, remedies and penalties"<sup>64</sup>. Similar general provision is included also in the Enforcement Directive (article 3) but still there is a specific reference to proportionality in the provision of the corrective measures<sup>65</sup>. Article 6 par. 3 ACTA applies to all remedies and thus it is fully applicable in the case of these remedies too.

- 
- (a) recall from the channels of commerce,
  - (b) definitive removal from the channels of commerce, or
  - (c) destruction".

The disposal outside the channels of commerce of the civilly infringing goods is provided also for TRIPs Agreement as an alternative to their destruction (Article 46).

- 62. The destruction is provided as a civil sanction, therefore the injured party must specifically claim destruction, while in criminal and administrative proceedings it may be ordered by the competent court/administrative authority ex officio.
- 63. The Anti-Counterfeiting Trade Agreement (ACTA): An Assessment, European Parliament, p. 27.
- 64. See also ACTA - Consolidated Text prepared for Public Release, April 2010 online at <[http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc\\_146029.pdf](http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf)> /accessed 01.09.2011, p. 7, Article 2.3, fn. 16.
- 65. Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 3.

As it was disclosed by the Commission during ACTA negotiations, parties agreed not to make additional references to the proportionality principle in other provisions of ACTA because an a contrario interpretal could not be based a contrario interpretation could be based whenever a specific reference was lacking<sup>66</sup>.

Another point to be made in relation to these other remedies is the definition of 'pirated copyright goods' which determines the extent of the application of those measures. The definition is given in section 2, article 5 (k) ACTA, which in conjunction with this article could lead to the interpretation that these measures may not be linked with an actual infringement in the territory of the EU where the action (e.g. destruction) is sought and it would be enough that the act "would have constituted an infringement". This wording could provide a possibility to destroy goods produced abroad when there has not been an actual infringement in the EU. And this because the definition of the 'pirated copyright goods' may create a legal fiction of an infringement in cases where no such infringement has been committed. Otherwise it would not be possible for the customs to intervene, because import as such does not constitute a copyright infringement. It was the intention of the Commission to correct this 'technical problem' during the last legal scrubbing of the text and the provision in question to read as the following: "At least with respect to goods that have been found to be pirated or counterfeited, each Party shall provide ..." <sup>67</sup>. Apparently the Commission was not able to impose this correction during the last negotiations.

Moreover, ACTA does not include the condition of TRIPs that the remedy of destruction should occur, "unless this would be contrary to existing constitutional requirements". Nonetheless, it can be interpreted that this could be one of the "exceptional circumstances" that are exempted from the provision's application, as "exceptional circumstances" form a kind of an exception.

Thus, there is no conflict between those measures provided for in ACTA and in EU law.

### **Right of information**

In the Opinion of the European Academics is also supported that the right of information provided in article 11 ACTA includes neither the proportionality requirement available under article 8 par. 1 of the Enforcement Directive nor effective protection against misuse of acquired information compared to article 8 par.

---

66. Commission Services Working Paper, p. 8 and Ficsor, slide 36.

67. European Commission, Note for the Attention of the Members of the Trade Policy Committee, 4.11.2010 TRADE E/PVM (2010), p. 6.

3(c) of the same Directive<sup>68</sup>. ACTA, however, contains a preemption rule for the national legislations on the protection of the confidential information, personal data and on statutory privileges, including the attorney privilege (article 11)<sup>69</sup>.

Additionally, ACTA provides the right of information against the infringer or the alleged infringer but not against third parties, contrary to article 8 of the Enforcement Directive (“any other person who (a) was found in possession of the infringing goods on commercial scale (b) was found to be using the infringing services on commercial scale.”). The group of persons that can be ordered to provide information goes beyond the infringer<sup>70</sup>. The difference between ACTA and Enforcement Directive is that the latter permits such information to be requested by third parties, such as the ISPs, only regarding activities carried out on ‘commercial scale’, meaning that consumers are excluded<sup>71</sup>. ACTA gives only the possibility in Section 5 to the authorities to order an ISP to disclose expeditiously to a rightholder information sufficient to identify a subscriber in accordance to article 27 par. 4 ACTA. Thus, ACTA provisions are less demanding than the EU acquis; the inclusion of ‘alleged infringers’ in article 11 aims to cover situations where the infringer is not yet condemned but still the relevant information is needed in the context of an ongoing judicial procedure (e.g. in provisional measures)<sup>72</sup>. The relevant information may include “information regarding any person involved in any aspect of the infringement or alleged infringement and regarding the means of production or the channels of distribution of the infringing or allegedly infringing goods or services, including the identification of third persons alleged to be involved in the production and distribution of such goods or services and of their channels of distribution”.

Relevant are also the ‘Privacy and Disclosure of Information’ statements contained in article 4 ACTA. These are intended to interact with and potentially limit the requirements for disclosure of information in article 11 (but also in article 22 ACTA). article 4 pars. 1(b) and (c) state clearly that ACTA gives the possibility to parties to preserve existing confidential information either for “public interest” or for “legitimate commercial interests of particular enterprises”. It leaves it though at the discretion of the parties to define those terms and consequently to the potential

---

68. Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 5.

69. Metzger, p. 113.

70. Accompanying document to the Report on the application of Directive 2004/48 on the enforcement of Intellectual property rights SEC(2010) 1589 final 22.12.2010, p. 10.

71. Accompanying document to the Report on the application of Directive 2004/48 on the enforcement of Intellectual property rights SEC(2010) 1589 final 22.12.2010, p. 10.

72. Commission Services Working Paper, p. 15.

political pressure exercised at bilateral level by other parties of the Agreement. Disclosure of information is a crucial element not only for civil and criminal enforcement but as well as for the enforcement on the digital environment and for border measures<sup>73</sup>.

Finally, another allegation against ACTA is that the regulated right of information is compulsory, while the right of information provided in TRIPs (Article 47) optional<sup>74</sup>. The character of this right in the European *acquis* is though also compulsory.

### Provisional measures

ACTA provides for provisional measures to prevent an infringement<sup>75</sup>, to prevent goods that involve the intellectual property right's infringement from entering into the channels of commerce, and to preserve relevant evidence in regard to the alleged infringement (article 12 par. 1). Additionally, ACTA provides the possibility these provisional measures to be taken *inaudita altera parte* (article 12 par. 2)<sup>76</sup>, without mentioning anything though about the necessary legal safeguards for the alleged infringer, as the Enforcement Directive (article 9 par. 4<sup>77</sup>) and TRIPs (article 50 par. 4<sup>78</sup> and 6<sup>79</sup>) do, i.e. that the parties should be informed without delay after the execution of the measures at the latest and that the defendant has the right of review, including a right to be heard, in order to be decided whether the

73. The Anti-Counterfeiting Trade Agreement (ACTA): An Assessment, European Parliament, p. 51.

74. Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 5.

75. In the Enforcement Directive the infringement is characterized as 'imminent' (Article 9 par. 1).

76. An *inaudita altera parte* or *ex parte* injunction is one having been granted without the adverse party having had notice of its application, and generally an application made by one party to a proceeding in the absence of the other, Gifis, *Steven Law Dictionary*, 1996 Barron's, p. 184.

77. "... In that event, the parties shall be so informed without delay after the execution of the measures at the latest. A review, including a right to be heard, shall take place upon request of the defendant with a view to deciding, within a reasonable time after notification of the measures, whether those measures shall be modified, revoked or confirmed".

78. "Where provisional measures have been adopted *inaudita altera parte*, the parties affected shall be given notice, without delay after the execution of the measures at the latest. A review, including a right to be heard, shall take place upon request of the defendant with a view to deciding, within a reasonable period after the notification of the measures, whether these measures shall be modified, revoked or confirmed".

79. "Without prejudice to paragraph 4, provisional measures taken on the basis of paragraphs 1 and 2 shall, upon request by the defendant, be revoked or otherwise cease to have effect, if proceedings leading to a decision on the merits of the case are not initiated within a reasonable period, to be determined by the judicial authority ordering the measures where a Member's law so permits or, in the absence of such a determination, not to exceed 20 working days or 31 calendar days, whichever is the longer".

measures will be modified, revoked or confirmed<sup>80</sup>. The right to be heard is not only a 'good to have' right but it is a fundamental right recognized in Article 6 European Convention on Human Rights (ECHR), in article 47 charter of fundamental Rights and guaranteed by the Court of Justice of the European Union<sup>81</sup>, even in the case of binding for the EU international law instruments, that do not include adequate precautions<sup>82</sup>. It is important to "ensure that a balance is maintained between the competing rights and obligations of the rightholder and of the defendant"<sup>83</sup>. Although in ACTA no such specific procedural safeguards exist at the adoption of provisional measures *inaudita altera parte*, it is provided however in article 6 that procedures enforcing the protection of IPRs should be applied "in such a manner as to ... provide for safeguards against their abuse" and that "procedures adopted, maintained, or applied to implement the provisions of this chapter shall be fair and equitable, and shall provide for the rights of all participants subject to such procedures to be appropriately protected" (article 6 par. 2). These guarantees apply to the entire chapter II and consequently to article 12 also. The lack of specific procedural safeguards in this case does not lead to the conclusion that this provision is inconsistent with the *acquis*, especially since nothing in ACTA challenges the procedural guarantees foreseen in the European *acquis*<sup>84</sup>. Besides ACTA's aim is not to regulate in every detail all the procedural details but "Each Party shall be free to determine the appropriate method of implementing the provisions of this Agreement within its own legal system and practice". Finally, in the very first Article of ACTA is stated that nothing in ACTA shall derogate from any obligation under existing agreements, including TRIPs. Thus, the relevant provisions of TRIPs (Article 50 par. 4 and 6) and the ones of the Enforcement Directive that implement the above mentioned provisions in the European legislative framework (Article 9 par. 4 and 9 par. 5) actually continue to apply<sup>85</sup>.

ACTA specifies that those provisional measures may be ordered by the judicial authorities, "where appropriate, against also a third party over whom the rele-

---

80. Additionally the Enforcement Directive requires that provisional measures to be revoked if the applicant does not institute proceedings leading to a decision on the merits of the case within a reasonable period of time (article 9 par. 5).

81. ECJ Case C-341/04, ECR 2006-I, 3813, para. 66, *Eurofood* and ECJ Case C-89/99, ECR 2001-I, 5851, Para. 38 seq. – *Schieving-Nijssatnd*.

82. Metzger, p. 113. ECJ, 28.03.2000, C-7/98, ECR 2000-I, 1935, para. 38 seq. *Krombach/Bamberški*.

83. ECHR App. No. 17506/06 para. 78 seq. – *Micallef/Malta* and Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 3.

84. Commission Services Working Paper, p. 8.

85. Commission Services Working Paper, p. 8 and Ficsor, slide 39.

vant judicial authority exercises jurisdiction". In the Enforcement Directive the third parties need to be involved in the infringement "against an intermediary whose services are being used"<sup>86</sup>. In ACTA the only precondition is the judicial authority to exercise jurisdiction over the third party against whom the provisional measures could be ordered.

It is important also to clarify the meaning of 'prevent from occurring' within the digital environment and if it would imply that the Internet Service Providers (ISPs) (third parties) must implement technical measures to prevent their customers from committing infringements. According to the Commission<sup>87</sup> 'prevent from occurring' in the digital environment in article 27 par. 1 ACTA also makes reference to "*expeditious remedies to prevent infringements*". This article is entirely consistent with the existing EU *acquis* in the field of intellectual property rights and also e-commerce. In particular, article 8 of Directive 2001/29, articles 3 and 9 of the Enforcement Directive and 12 par. 3, 13 par. (2) and 14(3) of Directive on e-commerce<sup>88</sup>. All these Directives provide the possibility for national authorities or courts to order provisional measures, by way the of injunctive relief to prevent or terminate an infringement of intellectual property rights in individual cases. An example of this situation would be a case where a court orders a website to remove advertisements promoting sales of counterfeit goods. ACTA does not introduce any requirement for technical measures in the context of article 27 par. 1 ACTA, pursuant at least with the European Commission's opinion<sup>89</sup>.

Hence, the provisions that foresee provisional measures in ACTA appear to be consistent with the Enforcement Directive.

### 3. Border measures

There were many voices that the implementation of ACTA would limit civil liberties and would allow the control of laptops or of air passengers at borders.

---

86. According to the Report on the Application of Directive 2004/48 COM(2010) 779, final, 22.12.2010, even intermediaries with no direct contractual relationship or connection with the infringer are subject to those measures provided for in the Enforcement Directive, p. 6.

87. Answer given by Mr De Gucht on behalf of the Commission (25.11.2010) P-9028/10EN online at <<http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2010-9028&language=EN>> /accessed 01.09.2011.

88. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services in particular electronic commerce in the Internal Market (Directive on Electronic Commerce), OJ L 178, 17.7.2000, p. 1-16.

89. Answer given by Mr De Gucht on behalf of the Commission (25.11.2010) P-9028/10EN online at <<http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2010-9028&language=EN>> /accessed 01.09.2011.

According to the Joint Declaration of 16 April 2010<sup>90</sup> there was no proposal to oblige ACTA participants to require border authorities to search travelers' baggage or their personal electronic devices for infringing materials.

An example of respecting fundamental freedoms is the *de minimis* clause in the Customs Regulation 1383/2003<sup>91</sup> that exempts travelers from checks, if the infringing goods are not part of a large scale traffic. But finally the *de minimis* exemption was not imposed as an obligation in ACTA, since ACTA leaves the opportunity to the contracting parties to opt out and recognize the right of other parties to carry out such boarder searches: "A party may exclude from the application of this section small quantities of goods of a non-commercial nature contained in traveler's personal luggage" (article 14 par. 2 ACTA). It worth's to be mentioned also that the relevant *de minimis* clause of Regulation 1383/2003<sup>92</sup> refers to goods "within the limits of the duty-free allowance" and it is unclear whether the 'small quantities' referred to ACTA are covered or not.

Similar *de minimis* rule is included also in TRIPs (article 60)<sup>93</sup>. Nevertheless, although TRIPs permits parties to exclude goods sent in small consignments, ACTA provides that the parties apply border measures to "goods of a commercial nature sent in small consignments" (article 14 par. 1 ACTA). Thus, ACTA emphasizes the commercial nature of the goods and not the size of the shipment and consequently urges the border authorities to apply the IP laws even to small shipments, leaving it up to the usually untrained border agent to determine whether the nature is commercial or not<sup>94</sup>. The *de minimis* provision seem to be on the one hand voluntary and on the other hand more restricted than in the European *acquis* and in TRIPs.

ACTA thrives to make the whole procedure easier for the rightholders in many different ways, than in the EU Regulation. In the first place, Regulation

---

90. Joint Statement on Anti-Counterfeiting Trade Agreement (ACTA) (16.04.2010) online at <[http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc\\_146021.pdf](http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146021.pdf)> /accessed 01.09.2011.

91. Council Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights OJ L 196, 02/08/2003, p. 7.

92. "Where a traveller's personal baggage contains goods of a non-commercial nature within the limits of the duty-free allowance and there are no material indications to suggest the goods are part of commercial traffic, Member States shall consider such goods to be outside the scope of this Regulation". Article 3 par. 2 Regulation 1383/2003.

93. "Members may exclude from the application of the above provisions small quantities of goods of a non-commercial nature contained in travelers' personal luggage or sent in small consignments".

94. Kaminski, p. 14.



1383/2003 requires from a rightholder lodging for an application to “have sufficient grounds for suspecting that goods infringe an intellectual property right” (article 4 par. 1), while ACTA demands from the rightholder to provide adequate evidence to demonstrate *prima facie* an infringement of the intellectual property right belonging to him. Most importantly though the last sentence of article 17 par. 1 ACTA lowers the standards for adequate evidence by providing that “the requirement to provide sufficient information shall not unreasonably deter recourse to the procedures”. Another weapon in the quiver of the rightholders is the possibility to provide for such applications to apply to multiple shipments (article 17 par. 2 ACTA)<sup>95</sup>.

Despite the differences that exist with regard to border measures between the European *acquis* and ACTA, the new Agreement does not impose any changes to the Directive 1383/2003, since all the distinct regulations in ACTA are not of mandatory character, permitting the Signatories to regulate it differently.

#### 4. Criminal enforcement

Another issue in ACTA that triggered many discussions and concerns -at least within the European Union sphere- is the criminal enforcement (section 4-Chapter II)<sup>96</sup>. The reason for these concerns was mainly the fact that the *n l' acquis communautaire* doesn't exist exists for criminal measures.

The efforts of EU to establish common internal standards of IPRs in the past were unsuccessful: first in the Enforcement Directive<sup>97</sup> and then in the so called IPRED

---

95. Kaminski, p. 16.

96. Section 4 of ACTA is about 'Criminal Enforcement' and contains four articles with provisions on 'Criminal Offences' (Article 23), 'Penalties' (Article 24), 'Seizure, Forfeiture, and Destruction' (Article 25) and 'Ex Officio Criminal Enforcement' (Article 26). Issues discussed during the negotiations under this Chapter included: clarification of the scale of infringement necessary to qualify for criminal sanctions in cases if trademark counterfeiting and copyright and related rights piracy, of the scope of criminal penalties, the authority to order searches and/or seizure of goods suspected of infringing IPRs, materials and implements used in the infringement, documentary evidence and assets derived from or obtained through the infringing activity, the authority of judicial authorities to order the forfeiture and destruction of the infringing goods and of the assets derived from or obtained through the infringing activity, Luc Pierre Devigne, Pedro Valasco-Martins & Alexandra Iliopoulou, Where is ACTA taking us? Policies and Politics, in Copyright Enforcement and the Internet (ed I. Stamatoudi), Kluwer Law International 2010, p. 37.

97. The criminal enforcement section was finally omitted from the Enforcement Directive in order to meet the deadline (May 1, 2004) of the Fifth Enlargement of the European Union.

2 Proposal for a Directive<sup>98</sup>. The last attempt started in 2005 and stalled for many years due to substantial differences among member states and due to problems concerning the legal basis. After the Lisbon Treaty, that entered into force on December 2009, the competence issue constitutes no longer a concern and it is shared between the Council and the European Parliament, based on article 83 par. 2 TFEU<sup>99</sup>. But still, the Commission on September 2010 has silently withdrawn the IPRED 2 proposal<sup>100</sup>.

Back to ACTA, apart from the issue of substance, which will be later analyzed, there was also a critical competence issue, *i.e.* who and whether was competent amongst the European institutions to negotiate ACTA concerning the criminal measures. Similar cases have existed in the past and EU committed to penal enforcement rules in international agreements, such as the TRIPs Agreement (article 61)<sup>101</sup>.

The European Community did not sign TRIPs criminal measures, because it was not competent. In its Opinion 1/94 of 15 November 1994<sup>102</sup> the European Court

---

98. Proposal for a European Parliament and Council Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights COM/2005/0276 final – COD 2005/127 \*/ online at <[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0276\(01\):EN:NOT](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0276(01):EN:NOT)>/accessed 01.09.2011.

99. “If the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures, directives may establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned. Such directives shall be adopted by the same ordinary or special legislative procedure as was followed for the adoption of the harmonisation measures in question, without prejudice to Article 76”.

100. Withdrawal of obsolete commission proposals 2005/0127/COD(2), OJ C 252, p. 9, 18.9.2010.

101. Answer given by De Gucht on behalf of the Commission 7.12.2010, E-8295/2010 online at <<http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-8295&language=EN>>/accessed 01.09.2011 and Commission Services Working Paper, Comments on the “Opinion of European Academics on Anti-Counterfeiting Trade Agreement”, 27.04.2011 online at <[http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc\\_147853.pdf](http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc_147853.pdf)>/accessed 01.09.2011, p. 11. The only difference is that ACTA goes beyond Article 61 of TRIPS by introducing additional definitions or interpretations of existing TRIPS obligations, by strengthening existing obligations, by removing existing flexibilities and by introducing new obligations for criminal enforcement (see analytically Henning Grosse Ruse-Khan, From TRIPS to ACTA: Towards a new ‘Gold standard’ in criminal IP enforcement?, Max Planck Institute for IP, Competition & Tax Law Research Paper Series, No. 10-06, p. 12-13). The European Academics on the other hand claim that ACTA is by nature outside the EU law and would require additional legislation on the EU level, Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 4.

102. Opinion of the Court of 15 November 1994. - Competence of the Community to conclude international agreements concerning services and the protection of intellectual

of Justice<sup>103</sup> developed further its ERTA<sup>104</sup> doctrine by pointing out that the Community's exclusive external competence does not automatically flow from its power to lay down rules at internal level and that only in so far as common rules have been established at internal level does the external competence of the Community become exclusive. Thus, the Opinion concluded that "as regards intellectual property, the harmonization achieved within the Community in certain areas covered by the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) is either partial or non-existent. With regard to the measures to be adopted to secure the effective protection of intellectual property rights, the Community is certainly competent to harmonize national rules on those matters pursuant to Article 100 of the Treaty, but the Community institutions have hitherto scarcely exercised their powers in that field. It follows that the Community and its Member States are jointly competent to conclude TRIPs"<sup>105</sup>. The Opinion did not refer to criminal measures but it has maintained the competence of the member states in sensitive areas for which no Community legislation had been adopted. As to the substance, the content of the Opinion supports 'mixture of competences'<sup>106</sup>.

---

property - Article 228 (6) of the EC Treaty. - Opinion 1/94. European Court reports 1994 Page I-05267 online at <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:61994V0001:EN:HTML>>/accessed 01.09.2011. See also relevant analysis at Meinhard Hilf, The ECJ's Opinion 1/94 on the WTO – No Surprise, but Wise?, 6 EJIL (1995) 1-259.

103. The questions put to the ECJ by the Commission in its request for an Opinion seek to ascertain, first, whether or not the Community has exclusive competence to conclude the Multilateral Agreements on Trade in Goods. Those questions further relate to the exclusive competence the Community may enjoy, to conclude the Agreement on Trade-Related Aspects of Intellectual Property Rights, including trade in counterfeit goods.
104. The creation of the doctrine is found in the ERTA case ECJ, Case 22/70 *Commission v. Council (ERTA)* [1971] ECR 263, para. 19. The case stated that the Community is competent to enter into international agreements with third States, but did more importantly introduced the doctrine of implicit competences, parallelism otherwise called the *ERTA-doctrine*. The case was about the Community's entry into an international agreement regulating road transports, an area in which the Community lacked expressed external powers. This did however not confine the Court, which states that the EC could have treaty-making capacity even in cases where such competences were not explicitly provided in the Treaty, Ott & Wessel, The EU's External Relations Regime: Multilevel Complexity in an Expanding Union, Working Paper Universiteit Maastricht (2005), Ch. 2.
105. Opinion of the Court of 15 November 1994.
106. Meinhard Hilf, The ECJ's Opinion 1/94 on the WTO – No Surprise, but Wise?, 6 EJIL (1995) 1-259, p. 13.

Similar approach was adopted also during the ACTA negotiations and for this reason was unnecessary to ask also in this case an opinion on ACTA from the Court of Justice of European Union, since probably the conclusion of the Court of Justice would not differ substantially from the WTO Opinion. In April 2008 the Council authorised the Commission to negotiate ACTA, pursuant to the Article 207 TFEU<sup>107</sup> (then article 133 of the EC Treaty) and agreed that the rotating Presidency of the EU, on behalf of the member states, would fully participate in the negotiations -in co-ordination with the Commission- on matters falling within member states competence. Such matters included the type and level of criminal penalties to be applied by ACTA Parties for infringements of IPRs and dispositions on penal procedural law<sup>108</sup>.

The non existence of *acquis* on criminal enforcement of IPRs seem -at least at the first place- to contradict two basic arguments of the European Commission for ACTA defense: a) That there would be no infringement of the *acquis communautaire* through the adoption of ACTA and b) that ACTA is not about substantive law but about enforcement of existing law, and this is why the *acquis communautaire* will remain unchanged. At the heart of ACTA anxiety is the danger of legislation through the back door and this is the point regarding the enforcement of criminal measures<sup>109</sup>.

The Commission's chief negotiator in ACTA, Luc Devigne, stated in a hearing on March 22, 2010<sup>110</sup> that, since the issue of criminal enforcement was not harmonized through a European Directive or in a different way, legal harmonization through ACTA would not be problematic, as it would not change the *acquis*. The Commission supports also the opinion that the criminal enforcement chapter of ACTA will not replace the need for a European *acquis* harmonizing the penal aspects of IPRs infringement. If we would accept that ACTA conflicts with EU law, because there are no provisions on criminal enforcement within the EU legal en-

---

107. See before Fn. 33.

108. Answers given by De Gucht on behalf of the Commission 30.11.2010, P-9029/10EN online at <http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2010-9029&language=EN>, 7.12.2010, E-8295/2010, online at <http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-8295&language=EN> and 15.03.2010, E-0217/2010, online at <http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-0217&language=EN>/all accessed 01.09.2011.

109. Lassi Jyrkkio, Smooth Criminal Harmonisation: ACTA, EU and IPR Enforcement, IP-Watch 8-4-2010 online at <http://www.ip-watch.org/weblog/2010/04/08/smooth-criminal-harmonisation-acta-eu-and-ipr-enforcement>/accessed 01.09.2011.

110. See details at <http://trade.ec.europa.eu/doclib/press/index.cfm?id=517>/accessed 01.09.2011.

forcement, then TRIPs could face -or should have faced- the same challenge (due to Article 61) as well. In the same way that no additional legislation was needed to implement the relevant provision of TRIPs, no special legislative measures need to be taken in regard with the criminal enforcement Section in ACTA<sup>111</sup>.

From the substantial issues the one that gathered the most concerns in the Chapter of 'Criminal Enforcement' was the definition of 'commercial scale'. According to Article 23 par. 1 ACTA and for the purposes for the section 4 "acts carried out on commercial scale include at least those carried out as commercial activities for direct or indirect economic or commercial advantage"<sup>112</sup>. The European opponents of ACTA support<sup>113</sup> that this definition contradicts the definition that was given in the proposal of IPRED 2 Directive, which expressly excluded acts "carried out by private users for personal and not-for-profit purposes"<sup>114</sup>. This proposal for a Directive, however, never came official to life and it has been recently abandoned. Thus, it has not been adopted and it does not belong to the EU *acquis*, as correctly indicates the Commission Services Working Paper (Comments on the Opinion of European Academics on Anti-Counterfeiting Trade Agreement)<sup>115</sup>. On the other hand the Commission has repeatedly stated that they took as basis for the negotiations the Study made for the Proposal for a Directive on criminal enforcement of IPRS (COM 2006/168 final).<sup>116</sup> Surprisingly -or not- nothing is

---

111. Commission Services Working Paper, p. 11.

112. The final text of ACTA has abandoned the previous formulation of this Article, in which 'commercial scale' was defined as including "a) significant willful copyright or related rights infringements that have no direct or indirect motivation of financial gain and b) willful copyright or related rights infringement for purposes of commercial advantage of financial gain". Consolidated text prepared for Public Release, ACTA April 2010 online at [http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc\\_146029.pdf](http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf) /accessed 01.09.2011. The omission of the 'significant' infringement lead probably to the expression of the present version of ACTA that acts carried out on commercial scale include 'at least' those ones carried out as commercial activities for direct or indirect economic or commercial advantage.

113. Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 4.

114. Position of the European Parliament adopted at first reading on 25.4.2007 with a view to the adoption of Directive on the harmonization of criminal measures aimed at ensuring the enforcement of intellectual property rights.

115. Commission Services Working Paper (Comments on the Opinion of European Academics on Anti-Counterfeiting Trade Agreement) online at [http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc\\_147853.pdf](http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc_147853.pdf) published in 27.04.2011 /accessed 01.09.2011, p. 12.

116. Answers given by De Gucht on behalf of the Commission 09.03.2010, O-0026/10EN online at <http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20100309>

mentioned in this Study concerning the above quoted exclusion from the scope of the Directive of acts “carried out by private users for personal and not-for-profit purposes” but only article 61 TRIPs is referred. The wording of article 23 par. 1 ACTA is compatible with article 61 TRIPs<sup>117</sup> because it provides that acts carried out on commercial scale include at least those carried out as commercial activities for direct or indirect economic or commercial advantages. The acts of commercial scale are not equal to acts committed for commercial purposes. Moreover, the interpretation by the WTO Panel confirms that the acts committed on a ‘commercial scale’ include also acts committed without commercial purposes but which -due to their magnitude or extent- reach the level of ‘commercial scale’<sup>118</sup>.

It has been supported that the qualification of ‘commercial scale’ has been reduced by ACTA to a mere qualitative element requiring a purpose of an economic or commercial advantage<sup>119</sup> and this contradicts the approach adopted by a WTO Dispute Panel has been regarding article 61 TRIPs, demanding both a qualitative and a quantitative element in order the notion of commercial gain to be established<sup>120</sup>. The definition in ACTA emphasizes more the qualitative element but it does not necessarily disqualify the quantitative character, since the phrase ‘at least’ pushes back this interpretation.

‘Commercial scale’ is a prerequisite for criminal liability and the visible concern for the definition of ‘commercial scale’ is that covers many activities that most people would not think that are of commercial nature. How does this prerequisite of ‘commercial scale’ apply to online infringement? The indirect economic advantage could cause major troubles, since it criminalizes a wide range of acts, other than the direct sales of infringing goods. It could be so interpreted, that it includes benefits as advertising revenues or even the prevention of expenditures or even shipping infringing goods, receiving in this way an indirect economic advantage<sup>121</sup>. Widespread file sharing between individuals could be interpreted as ‘commercial scale’ especially after the omission of an EU-like expression that

---

&secondRef=ITEM-015&language=EN>/accessed 01.09.2011 and on 27.09.2010, E-4292-/10EN online at <<http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-4292&language=EN>>/accessed 01.09.2011.

117. The non-derogation provision of Article 1 par. 1 of ACTA should be also kept in mind.

118. WTO Dispute Settlement Understanding (DSU) USA against China (WT/DS362/R, 09/O240, 26.01.2009) (China-IPRs) and Ficsor, slide 59.

119. Henning Grosse Ruse-Khan, p. 14.

120. WTO Dispute Settlement Understanding (DSU) USA against China (WT/DS362/R, 09/O240, 26.01.2009) (China-IPRs) regarding *inter alia* Article 61 TRIPs (WTO, 2009) at 7.544-7.552, 7.577.

121. Kamiski, p. 18.

would exclude expressly any acts carried out by end consumers acting in good faith. Generally, it could be argued that the concepts used to define commercial scale are relatively unclear and they do not provide for an appropriate and sufficiently precise definition of the element of a crime under the current laws in the EU. The definition though is based on the commercial activity which will be interpreted and implemented by the domestic legislation and the jurisprudence of the parties<sup>122</sup>.

It is also important to mention that in the EU acquis already exists a definition of 'commercial scale' not in the context of criminal measures but in the Enforcement Directive. According to preamble (recital 14) "Acts carried out on a commercial scale are those carried out for direct or indirect economic or commercial advantage..." and this definition presents quite a resemblance with the one in ACTA. The definition in the preamble of the Enforcement Directive, however, continues clarifying that "this would normally exclude acts carried out by end consumers acting in good faith"<sup>123</sup>. This clarification is absent from ACTA and although this could be detrimental for the consumers, since the borderline between commercial and non-commercial use is often very difficult to be distinguished, it does not lead to the conclusion that the EU does not have the possibility to add this in any future definition of 'commercial scale' with regard to criminal enforcement measures.

Apart from that, it has been also claimed that ACTA does not affirm safeguards for private users and for limitations and exceptions, because there is no provision regulating that any act that would qualify as an exception would not constitute a criminal offence (similar provision was included in the proposal for the IPRED 2 Directive by the European Parliament)<sup>124</sup>. Nevertheless, the legitimate exceptions stay out of the spectrum of criminal enforcement of ACTA, which applies only to willful illegal activities (such as piracy and counterfeiting) practiced on a 'commercial scale'<sup>125</sup>.

Finally, in regard to the safeguards for ensuring the balance of interested parties, the opponents of ACTA claim that are not provided for in the text, and the same applies to the infringer's right to be heard in the procedures of seizure, forfeiture and destruction<sup>126</sup>. We have to keep in mind though, that on the one hand the general provision on safeguards and procedural guaranties in article 6 par. 2

---

122. Commission Services Working Paper, p. 18.

123. Commission Services Working Paper, p. 12.

124. Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 4.

125. Commission Services Working Paper, p. 12.

126. Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 4.

ACTA applies also to the Chapter of criminal enforcement and that on the other hand ACTA will not repeal the safeguards already foreseen in the national legislation of the Parties or the European Union legislative framework<sup>127</sup>.

### Camcording

ACTA additionally criminalizes unauthorized filming movies in movie theaters (the so called camcording) (article 23 par. 3 ACTA). The inclusion of this undertaking within the acts that a Party may provide criminal procedures is due probably to the USA, that has enacted already in 2003 the U.S. Camcorder ACT<sup>128</sup>. No specific anti-camcord legislation exists in the European Union but for Italy and Spain, yet there is coverage under other relevant laws<sup>129</sup>. Although the criminalization of the act of “unauthorized copying of cinematographic works from a performance in a motion picture exhibition facility generally open to the public” seem to be possible without the ‘commercial scale’ assessment and without any assessment of the intention of the infringer, it is positive that it is merely optional for the Parties of ACTA. This is also why this provision does not conflict with the European acquis. Moreover according to the European Commission the copyright exceptions are not covered by ACTA and thus, the private copy exceptions still apply<sup>130</sup>.

It has been argued that although the optional character of camcording’s criminalization was a positive development, it is not equally encouraging the fact that judges in ACTA countries could still order seizure, forfeiture, and destruction of DVDs containing camcorded movies, or equipment used in camcording (article 25)<sup>131</sup>. This position is not correct, because article 25 ACTA provides that “With respect to the offences specified in paragraphs 1,2,3, and 4 of Article 23 (Criminal Offences) for a which a party provides criminal procedures and penalties ...” making it clear that the Party has the possibility to provide the competent authorities to have the authority to order the seizure, the forfeiture and the destruction of the pirated copyright goods, only regarding acts for which criminal offences are provided. Since the criminalization of camcording is optional, in the case where no criminal offence is provided, no seizure, destruction or forfeiture can be imposed.

---

127. Commission Services Working Paper, p. 13.

128. The Family and Entertainment Act of 2003, 18 U.S.C. § 2391B (2010) Unauthorized recording of motion pictures in a motion picture exhibition facility.

129. Anti-Camcord Legislation (ACL) Chart online at <<http://www.natoonline.org/pdfs/PDF%20Movie%20Theft/International%20Camcord%20Statutes.pdf>> /accessed 01.09.2011.

130. Commission Services Working Paper, p. 13.

131. Rashmi Rangnath, USTR releases finalized ACTA text: Concerns remain online at <<http://www.publicknowledge.org/blog/ustr-releases-finalized-acta-text-concerns-re>> /accessed 01.09.2011.



## 5. Safeguards

One of the alleged disadvantages of ACTA is the fewer safeguards that it includes, having eliminated safeguards available under TRIPs<sup>132</sup>. Without analyzing the concrete provisions, it has to be underlined in this regard that ACTA already in the preamble states that its purpose is complementary to TRIPs (Preamble par. 4) and the first article assures that its provisions are compatible with existing agreements, including TRIPs. Thus, all the mandatory safeguards provided for in TRIPs are in no way modified by ACTA, without being necessary to be mentioned and repeated specifically in the text of ACTA. EU member states must still comply with TRIPs and its safeguards.

Besides, the more general safeguards in TRIPs contained in articles 7 and 8 are incorporated in ACTA through article 2 par. 3. article 7 of TRIPs secures that the enforcement of IPRs “should contribute to the promotion of technological innovation and to the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations”. Article 8 par. 2 TRIPs<sup>133</sup> allows parties to provide measures to prevent the abuse of IPRs.

Also it should not be overlooked that other safeguards exist also in the preamble of ACTA, i.e. par. 5 expresses the goal that enforcement should not be implemented in a way that poses greater barriers to trade and par. 6 states that the problem of infringement of IPRs is desired to be addressed “*in a manner that balances the rights and interests of the relevant rightholders, service providers, and users*”.

Of particular importance are also the ‘Privacy and Disclosure of Information’ statements contained in Article 4 ACTA, already mentioned before. And finally there is always article 6 in the General Obligations, which provides a strong basis on which stakeholders can demand balanced implementation. Article 6 par. 2 of ACTA provides that procedures should be fair and that the rights of all participants should be protected. Those provisions are mandatory, which means that they must be given as much attention as other provisions of ACTA and that they are operative<sup>134</sup>.

---

132. Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 5.

133. “Appropriate measures, provided that they are consistent with the provisions of this Agreement, may be needed to prevent the abuse of intellectual property rights by rightholders or the resort to practices which unreasonably restrain trade or adversely affect the international transfer of technology”.

134. The Anti-Counterfeiting Trade Agreement (ACTA): An assessment, European Parliament, p. 51.

## ***6. Enforcement of intellectual property rights in the digital environment (Section 5)***

The most controversial chapter in ACTA and the one that triggered the most conversations within the academic and business fields is section 5, the enforcement of intellectual property rights in the digital environment. For the ones that did not follow closely the ACTA negotiations would be useful to notice that the version of this section finally adopted presents many differences than the previous ones. We will not analyze thoroughly the previous versions of this section and the relevant provisions, since this would exceed the needs of this paper. The basic provisions though will be mentioned and we will examine the meaning of the changes ultimately adopted regarding the enforcement in the digital environment and most importantly what is the role that the ISPs are called to play. Additionally the issue of technological measures is also considered.

Much of the controversy has been focused on the possibility that ACTA would require from the parties to enforce a graduated response system or also known as a 'three strikes system', in which ISPs are required to terminate internet access to their subscribers in the case of repeated copyright infringement. A few countries, amongst them also some European ones, such as France and UK, have already adopted or they are about to adopt graduate response mechanisms in their national legislations.

### **The non-adopted provision**

In the non-adopted version of the enforcement in the digital environment section ISPs could enjoy an immunity, so long as they had no direct responsibility for the infringement. This provision did not present any difference to the European *acquis* and specially to Directive on e-commerce. Nevertheless, there was a catch; the ISP safe harbors provisions presupposed that the ISPs should have adopted and reasonably implemented "a policy to address the unauthorized storage or transmission of materials protected by copyright". In order the meaning of this wording to be crystal clear a footnote was clarifying that an example of such policy could be "providing for the termination in appropriate circumstances of subscriptions and/or accounts in the service provider's system or network of repeat infringers"<sup>135</sup> a sic expression to describe the three strikes approach. A

---

135. See similar provision in the US Copyright law, Section 512(i) of the Digital Millennium Act (DMCA) "Conditions for Eligibility.— (1) Accommodation of technology.— The limitations on liability established by this section shall apply to a service provider only if the service provider— (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscrib-

second condition in order an ISP to enjoy immunity was the existence of a 'take-down' procedure, although no specific mechanism was definitely decided and a number of options mirrored the undecisiveness of the parties<sup>136</sup>. Generally, it could be said that many of the provisions of the older versions of this section of ACTA presented a definitive resemblance to DMCA and they were interpreted as an attempt to export the DMCA provisions to the international legal framework. On the one hand, however, the disagreements of many parties on the internet provisions and specifically the ISP liability and on the other hand the desire of USA to conclude the Agreement before the end of 2011, were probably the major reasons that the three strikes rule was finally dropped from ACTA and the so called 'ACTA Ultra-Lite' version was created and adopted<sup>137</sup>. Out of the text were liability exemptions and conditions to make ISPs eligible for such exceptions. The enforcement in the digital environment Section was diminished from five to three pages and the result was more protective to substantive rights, liabilities and exceptions<sup>138</sup>.

### The (finally adopted) section 5

In the final text of ACTA any reference to graduated response has been omitted. Nonetheless, footnote 13 offers the possibility to the parties to preserve or even to adopt any existing system providing for ISP liability limitation.<sup>139</sup> In the final version of ACTA there is only one provision in this regard, that provides for the following in article 27 par. 3: "Each Party shall endeavour to promote cooperative efforts within the business community to effectively address trademark and copyright or related rights infringement while preserving legitimate competition and, consistent with that Party's law, preserving fundamental principles such as freedom of expression, fair process, and privacy." The wording 'shall endeavour'

---

ers and account holders of the service provider's system or network who are repeat infringers; ...". This footnote was included in the Draft of January 18, 2010 (Informal Predecisional/Deliberative Draft), p. 28 n. 29 but was eliminated in the April Draft of ACTA.

136. ACTA Consolidated Text, April 2010, p. 21.

137. As the last version was named by Mr Hammerstein from the Trans-Atlantic Consumer Dialogue, Ermert, Treaty Negotiations turn to "ACTA-Lite" in hopes of Closure, IP Watch (8.9.2010) online at <<http://www.ip-watch.org/weblog/2010/09/08/treaty-negotiators-turn-to-%E2%80%9Cacta-lite%E2%80%9D-in-hopes-of-closure/>> /accessed 01.09.2011.

138. See analytically for the relevant provisions in the oldest version of ACTA at Bridy, ACTA and the Specter of Graduate Response, American University International Law Review, Vol. 26, No. 3, pp. 558-577, Spring 2011 PIJIP Research Paper No. 2, p. 3ff.

139. The Anti-Counterfeiting Trade Agreement (ACTA): An assessment, European Parliament, p. 57.

has replaced the 'shall' and the provision having only apparently a mandatory character does not impose any obligation to bring results and could not be interpreted as mandating ACTA Signatories to introduce 'three strike' or similar systems. Apart from this provision a new relevant statement made its entry in the preamble (par. 7) according to which the Parties to ACTA desire "... to promote cooperation between service providers and rightholders to address relevant infringements in the digital environment."

After the strong resistance and pressure from both within and outside the negotiation procedure the parties (and most importantly the USA who urged for an IP maximalism and pushed for stricter provisions) have compromised and abandoned the provisions regulating intermediary liability provisions. It seems that the aspirations of IP maximalists have been disappointed but this statement is not exactly true. The current provision does not constitute an obligation anymore to the Signatories of the Agreement and to the others that will entry in a later point but definitely it gives the means to the 'strong' and powerful parties to press for such a voluntary cooperation between service providers and rightholders. A mandatory provision obliging the governments to establish a three strike systems to the ISPs was expected to -and did- cause major reactions to the consumers, the ISPs and generally the public at large. On the contrary the change to a voluntary language had a calming down effect and on the same time supplied the means to push for the 'voluntary cooperation'. In any case this wording resonates strongly the industry demands that ISPs should take a more active role in antipiracy efforts in the digital environment. The strategy of the entertainment industry was either to establish the graduated response systems through legal instruments in the national legislation or, when this was not possible, to seek government pressure for graduated response or the three strike system<sup>140</sup>. ACTA seem to follow the recent trend away from a passive-reactive approach (requiring from carriers and hosts to behave passively until becoming aware of copyright-infringing activities on their networks) toward an active-preventative approach instead. Government policies, voluntary practices, legislative enactments, and judicial rulings are all contributing to this shift in the rules applicable to online intermediaries<sup>141</sup>.

The principle of cooperation between concerned parties and the seeking of voluntary solutions is not unknown in the European *acquis* and it is already foreseen

---

140. Bridy, at 10.

141. DeBeer Jeremy F. & Clemmer Christopher D. Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries? *online at* <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1529722](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1529722)> /accessed 01.09.2011.

in articles 15 par. 2, 16 (Codes of Conduct) and 19 (Cooperation) of the Directive on e-commerce as well as in article 17 of the Enforcement Directive<sup>142</sup>.

Additionally 27 par. 4 ACTA provides the possibility (prescribes no obligation to the Parties) to give the relevant authorities “the authority to order an online service provider to disclose expeditiously to a rightholder information sufficient to identify a subscriber whose account was allegedly used for infringement, where that rightholder has filed a legally sufficient claim of... copyright or related rights infringement, and where such information is being sought for the purpose of protecting or enforcing those rights These procedures shall be implemented in a manner that avoids the creation of barriers to legitimate activity, including electronic commerce, and, consistent with that Party’s law, preserves fundamental principles such as freedom of expression, fair process, and privacy”<sup>143</sup>.

The measures aimed at requiring ISPs and other intermediaries to provide information about subscribers to rightholders on request are not mandatory. The provisions mandating the application of normal procedures for injunctions and provisional measures are also applied in the enforcement in digital environment due to article 27 par. 1.

Article 27 par. 4 ACTA corresponds to existing EU legislation, in particular article 8 of the Enforcement Directive, that provides that ISPs may be ordered by competent judicial authorities to provide personal information, that they hold about alleged infringers (e.g. information regarding the origin of distribution networks of the goods or the services which infringe an intellectual property right) in response to a justified and proportionate request in cases of infringement on a commercial scale (see also the relevant Recital 14 of the Enforcement Directive). Thus, the ‘commercial scale’ is a decisive factor to determine the limits of

---

142. ACTA Debate European Parliament, 20.10.2010 online at <<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20101020+ITEM-016+DOC+XML+V0//EN>>/accessed 01.09.2011 and answer given by De Gucht on behalf of the Commission 22.12.2010, P-9026/10EN online at <<http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=P-2010-9026&language=EN>>/accessed 01.09.2011.

143. The ACTA provision on the disclosure of subscribers’ data (Article 27.4) is not mandatory and it cannot be compared with the different nature of Article 47 of TRIPs “Members may provide that the judicial authorities shall have the authority, unless this would be out of proportion to the seriousness of the infringement, to order the infringer to inform the rightholder of the identity of third persons involved in the production and distribution of the infringing goods or services and of their channels of distribution”. The scope of the provision is mostly to detect the business structures. Vander, in Busche/Stoll, TRIPs, 2007, Article 47 Rdn 3. In any case when TRIPs was negotiated in early 90’s ISPs were not unknown but definitely were not taken into account by the drafting of the provision, Commission Services Working Paper, p. 19.

the monitoring and to set the boundaries of respecting proportionality<sup>144</sup>. Similarly article 15 par. 2 of Directive on e-commerce provides that “Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements”.

As already stated before, the provision of article 27 par. 4 ACTA lays down a number of safeguards that “These procedures shall be implemented in a manner that avoids the creation of barriers to legitimate activity, including electronic commerce, and, consistent with that Party’s law, preserves fundamental principles such as freedom of expression, fair process, and privacy.” Thus, any implementation of this ACTA provision is subject also to the EU fundamental rights, namely the freedom of expression, fair process and privacy. It is reasonable that it cannot be expected from an international instrument to be as detailed as the national laws or even the European Directives. An international agreement, such as ACTA, is expected to give the general guidance and the key principles, which will be further elaborated by the national legislations<sup>145</sup>.

Another clause that safeguards the role of service providers and respects the rule of law is that rightholder must file “*a sufficient claim*” to disclose the information required. However, there is much room for legal interpretation on what constitutes a sufficient claim of infringement.

Also the general safeguards foreseen in ACTA should not be overlooked. Even in the footnote 13, which envisions the possibility for the Parties to maintain or to adopt limitations on the liability of ISPs, the need for preservation of the legitimate interests of the rightholders is emphasized.

As far as it concerns which authority is competent to order the disclosure of the information, both the EU legislation (article 15 par. 2 of the Directive on e-Commerce) and ACTA refer to the competent (public) authorities, which will have to be determined according to parties’ legislations. In the EU context and depending on the legal framework of each member state, these will be either judicial or administrative authorities. For instance, in the case of civil proceedings, Article 8

---

144. Opinion of European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), OJ 5.6.2010, C 147, p. 1.

145. Commission Services Working Paper, p. 19.

par. 1 of the Enforcement Directive clearly allocates this power to the competent judicial authorities<sup>146</sup>.

Within the EU it is also worth recalling the Amendment 138 to the framework Directive<sup>147</sup> in the context of review of Telecoms Package.<sup>148</sup> Most of the scope of the Telecoms Reform Package is of limited -or no- relevance here. Only Proposal 138 for the Better Regulation Directive is interesting for our topic and was the one most widely debated in media, in the EU Parliament and the Council. The final and compromised version of the Amendment replaced the requirement for a “prior ruling by the judicial authorities” with the requirement for a “prior fair and impartial procedure” in order measures to be taken regarding end-users access to electronic communications networks. In this provision (article 1 par. 3a)<sup>149</sup> it is laid down that any restriction to fundamental rights or freedoms may only be imposed if the measures are appropriate, proportionate and necessary within the democratic society and their implementation should be subject to adequate pro-

---

146. Answer given by Mr De Gucht on behalf of the Commission at parliamentary question P-9459/10EN (10.1.2011).

147. Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 OJ L 337, 18.12.2009, p. 37.

148. The Telecoms Reform Package was presented to the European Parliament on November 13, 2007, voted upon May 6, 2009 and finalized on November 25, 2009. It comprises of five Directives (the Framework Directive, the Access Directive, the Authorization Directive, the Universal Service Directive and the E-privacy Directive).

149. Article 1 par. 3a of Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002. “Measures taken by Member States regarding end-users access to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law. Any of these measures regarding end-users’ access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of the presumption of innocence and the right to privacy. A prior, fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to effective and timely judicial review shall be guaranteed”.

cedural safeguards in conformity with the ECHR and with general principles of EU Law including effective judicial protection and due process.

Thus, there is no conflict between ACTA and EU law in this Section. ACTA demands respect for the fundamental principles (as it is also dictated in the European directives) and each Party has to implement those principles in a more detailed manner in the national legislation.<sup>150</sup>

### TPMs

The anti-circumvention rules of ACTA have also significantly changed from the initial versions of the draft texts. In the final text of ACTA there are some additional requirements.

In order to provide the adequate legal protection and effective legal remedies referred to in article 27 par. 5, each party shall provide protection at least against:

“(a) to the extent provided by its law: (i) the unauthorized circumvention of an effective technological measure carried out knowingly or with reasonable grounds to know; and

(ii) the offering to the public by marketing of a device or product, including computer programs, or a service, as a means of circumventing an effective technological measure; and:

(i) the unauthorized circumvention of an effective technological measure carried out knowingly or with reasonable grounds to know; and

(ii) the offering to the public by marketing of a device or product, including computer programs, or a service, as a means of circumventing an effective technological measure;”

The crucial point is the phrase “*to the extent provided by its law*” which makes the requirements optional and it presupposes that they exist in a Party’s national legislation. In the case they are not found in the national law, it is not obligatory to implement these requirements.

Additionally another requirement that ACTA sets is that the technological protection measures (TPMs) are used by authors, performers or producers of phonograms in connection with the exercise of their rights, meaning that TPMs used by another group, such as broadcasters to control access to scheduled programmes are not protected, or TPMs used by a group of beneficiaries to achieve goals not

---

150. Ficsor, slide 63.



linked to protecting their copyright (access control) are not protected either.<sup>151</sup> The provision in the European *acquis* is more general and it does not have a language restricting the protected TPMs to the ones used by authors, performers or producers but applies to all rightholders of any copyright or any right related to copyright as provided for by law or even the *sui generis* right provided for in Directive 96/9/EC (article 6 par. 3 of the Information Society Directive 2001/29).

Regarding circumvention of TPMs ACTA (articles 27 pars. 5 and 6) has brought changes to the relevant international instruments regulating this topic, i.e. WCT and WPPT<sup>152</sup>. WCT requires Parties to “provide adequate legal protection ... against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights ... and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law”<sup>153</sup> Despite the resemblance between ACTA provisions (article 27 par. 5) and WCT, ACTA additionally gives a definition of technological measures in footnote 14<sup>154</sup> broadening international law specifying that the technological measures are deemed as ‘effective’ when works are controlled “through the application of a relevant access control or protection process, such as encryption or scrambling, or a copy control mechanism, which achieves the objective of protection”<sup>155</sup>. Although ACTA elaborates more the ways in which such protections should be extended, this does not constitute a problem for EU, since they remain within the framework of article 6 of the Information Society Directive, which implements articles 11 WCT and 18 WPPT.<sup>156</sup>

---

151. European Commission, Note for the Attention of the Members of the Trade Policy Committee, 4.11.2010 TRADE E/PVM (2010), p. 7.

152. To some extent anti-circumvention provisions are found in Articles 2, 3 and 6 of the Council of Europe Convention on Cybercrime online at <<http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>>/accessed 01.09.2011.

153. Article 11 WCT. See also article 18 WPPT.

154. For the purposes of this article, technological measures means any technology, device, or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works, performances, or phonograms, which are not authorized by authors, performers or producers of phonograms, as provided for by a Party's law. Without prejudice to the scope of copyright or related rights contained in a Party's law, technological measures shall be deemed effective where the use of protected works, performances, or phonograms is controlled by authors, performers or producers of phonograms through the application of a relevant access control or protection process, such as encryption or scrambling, or a copy control mechanism, which achieves the objective of protection.

155. Kaminski, p. 22.

156. Report on the application of the Directive on the harmonisation of certain aspects of copyright and related rights in the information society (2001/29/EC), 30.11.2007, SEC(2007)

Article 27 pars. 5 and 6 of ACTA seem to be in accordance with Article 6 of the Information Society Directive 2001/29<sup>157</sup>. Article 6 par. 2 of Information Society Directive prohibits a wide range of preparatory activities. As it has been supported<sup>158</sup>, article 6 of the Information Society Directive is based on a correct interpretation of the relevant provisions of the WCT and the WPPT. Without the prohibition of the preparatory acts the provisions of the Directive could not fulfill the obligation to provide adequate protection and effective remedies against circumvention of technological protection measures. It would also refuse protection to certain TPMs, which would be in conflict with the provisions of the Treaties requiring protection for any TPMs (both access-control and rights control)<sup>159</sup>. Some argue that ACTA goes beyond the relevant provisions of the WCT and the WPPT<sup>160</sup> but it cannot be supported that goes substantially beyond the relevant provision of the Information Society Directive, since the latter prohibits also preparatory acts.

Another point that raised concerns is the lack of a mechanism to ensure the exercise and enforcement of exceptions and limitations<sup>161</sup>. Nevertheless, ACTA in article 8 gives the possibility to a Party to “*adopt or maintain appropriate limitations or exceptions*” to measures implementing the prohibition of circumvention of TPMs and the protection of electronic management information. At the same time ACTA preserves the *status quo* of the rights, limitations and exceptions or defenses to copyright or related rights infringement existing in the law of a party. This general approach is due to the different national legislations, since not all ACTA parties have ratified WIPO Internet Treaties<sup>162</sup>. So, actually concerning TPMs ACTA (article 27 par. 8) preserves the right of the Parties not only to maintain any possible existing exceptions and limitations but also to adopt new ones, if they consider it necessary. Accordingly, the European *acquis* is maintained but questionable is if the crafting of new exceptions and limitations is allowed<sup>163</sup>.

---

1556 online at <[http://ec.europa.eu/internal\\_market/copyright/docs/copyright-info/application-report\\_en.pdf](http://ec.europa.eu/internal_market/copyright/docs/copyright-info/application-report_en.pdf)>/accessed 01.09.2011, p. 6.

157. In EU legislative framework anti-circumvention provisions can be found also in two more Directives; in Article 7 par. 1(c) of the Computer Programs Directive and in article 4 of the Conditional Access Directive.

158. Ficsor, slides 61 and 62.

159. Ficsor, slide 62.

160. Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 6.

161. Opinion of European Academics on the Anti-counterfeiting Trade Agreement, p. 6.

162. Commission Services Working Paper, p. 18-19.

163. The Anti-Counterfeiting Trade Agreement (ACTA): an assessment, European Parliament – Directorate-General for External Policies/Policy Department, p. 57.

This means that any anti-circumvention protection can be subject to any existing exceptions and there is no limitation on the scope of exception to TPMs<sup>164</sup>. This general approach to limitations and exceptions gives also the possibility to apply the relevant exceptions for computer programs (Directive 91/250)<sup>165</sup>.

Regarding interoperability and technical provision Footnote 15 solves any misconception stating that there is no obligation to amend the current legal framework, since there is no obligation for a Party to mandate interoperability and more specifically there is no obligation to ICT industry to design devices, products, components or services to correspond to certain technological measures. In this way the limitations expressed in Directive 2001/29 (Recital 48-second sentence) and in Directive 91/250 are maintained. To this aim a Negotiator's Note has been added for clarification at the request of EU.

### III. Conclusion

In the conclusion we are supposed to give an answer to the question posed in the title of the paper. Is there finally a love or a hate relationship between ACTA and copyright in the EU<sup>166</sup>? Or to put it in other words is ACTA compatible with the European *acquis communautaire* concerning copyright? The question is not only of academic value but also of a high practical importance. The ratification of the Treaty could depend on the answer given -not of course by the author of this paper but- by the European institutions and more importantly by the members of the European Parliament.

The fact that ACTA falls under Article 207 TFEU<sup>167</sup> means that the standard rules on ratification apply. The Commission will need to formally decide whether to propose the agreement for ratification and the Council will need to decide whether to sign and conclude the Agreement. Already on August 23, 2001 the EU Council has published Document 12192/11<sup>168</sup> conveying a draft Decision saying

---

164. In earlier drafts it was included that the limitations were permitted "so long as they do not significantly impair the adequacy of legal protection of technological measures or electronic rights management information or the effectiveness of legal remedies for violations of those measures", ACTA - Consolidated Text prepared for Public Release, April 2010, Article 2.18 (7) (6.2), p. 24.

165. It is the only section in ACTA where limitations and exceptions are explicitly mentioned.

166. For a history and current situation of copyright law in the European Union, See Spinello R. & Bottis M., A defence of intellectual property rights, 2009, pp. 26-30, 82-95.

167. Relevant also article 2 subsection 2 and Articles 216 et seq. TFEU.

168. Online at <<http://register.consilium.europa.eu/pdf/en/11/st12/st12192.en11.pdf>>/accessed 01.09.2011.

that the President of the Council shall be authorised to designate the person(s) empowered to sign the Agreement on behalf of the Union. To the extent that the agreement is mixed, *i.e.* it concerns both EU and Member States' competences, it will require ratification also by the Member States<sup>169</sup>. Finally, the Parliament will be required to give its consent. If ACTA requires changes in the EU *acquis*, this may incline a number of European Parliamentarians to vote against the ratification of the Treaty as it stands.

The final text does not seem to fulfill its initial aims to robust cooperation mechanisms among ACTA Parties to assist in their enforcement efforts, to establish best practices for effective IPR enforcement and to set clear 'state of the art' IP enforcement rules "in a manner that balances the rights and interest of the relevant rightholders, service providers and users". The final wording of ACTA is not as draconic as the first leaked drafts, since the most controversial parts have been abandoned or softened and for sure it does not justify the paranoia against ACTA<sup>170</sup>. The only positive element from this anti-ACTA hysteria was the raising of awareness about the issue of IPRs enforcement on general.

In the light of the analysis conducted, it can be supported that the provisions of ACTA seem to be in line with the EU *acquis communautaire*, at least with regard to copyright. Is this conclusion enough to state that there is a love relationship between ACTA and copyright law in EU? Probably not! It could be described as a tolerance or even an affinity relationship but in no way a love relationship, since ACTA brought neither the disaster that the laymen were afraid of nor the Land of Promise due to the compromises that reduced the force of Parties' obligations and led to an Agreement that fell short of the ambitious aims with which it begun.

---

169. The EC in the documents for a Council Decision, tabled on June 24, 2011 proposing the signature and conclusion of ACTA (COM(2011) 379 final, 2011/0166 (NLE) and COM(2011) 380 final, 2011/0167 (NLE)) recommended against any further review of ACTA before it is passed by the European Parliament. The proposal for a Council Decision on the conclusion of ACTA opens with an Explanatory Memorandum, noting that "the Commission has opted not to propose that the European Union exercise its potential competence in the area of criminal enforcement pursuant to Article 83(2) TFEU. The Commission considers this appropriate because it has never been the intention, as regards the negotiation of ACTA to modify the EU *acquis* or to harmonise EU legislation as regards criminal enforcement of intellectual property rights. For this reason, the Commission proposes that ACTA be signed and concluded both by the EU and by all the Member States" (cf. COM(2011) 379 final, 2011/0166 (NLE), page 3; COM(2011) 380 final, 2011/0167 (NLE), page 2).

170. See examples online at <http://www.stopacta.info/alertbox>, <<http://www.gamma.net.nz/content/sign-wellington-declaration>>/accessed 01.09.2011 and <[http://www.laquadrature.net/wiki/Help\\_sign\\_the\\_Written\\_Declaration\\_12/2010\\_about\\_ACTA](http://www.laquadrature.net/wiki/Help_sign_the_Written_Declaration_12/2010_about_ACTA)>/accessed 01.09.2011.

# The idea of legal convergence and electronic law

---

---

Antonios Platsas

---

---

## Introduction

This paper deals with the leading thesis in the discipline of law, the law convergence thesis. The thesis stands for the coming together of different legal systems. The thesis in question is negotiated herein with a focus on the subject-area of electronic law. I will approach a limited amount of legal systems and orders in the area by taking a macro-comparative approach. At the international level, I will question the reach of the relevant international law instruments. Most importantly, the paradox of the presence of a world-wide framework of electronic communications (the internet) and the parallel absence of world-wide regulatory frameworks will be highlighted and criticised. The paper will draw its analysis on the very nature of the internet, especially in the sphere of eCommerce, where there is now clear need for further global regulation.

## Convergence of Legal Systems

It is my conviction that the thesis which entails the coming together of different legal systems, traditions and mentalities (law convergence thesis) stands for the leading thesis in the discipline of law. The answer for the reasons behind this is readily available: whilst other disciplines have some time ago reached a consensus of epistemological unity, law still takes a rather parochial and introvert approach. Zweigert & Kötz's well-known quote is certainly illuminating here:

“There is no such thing as “German” physics or “British” microbiology or “Canadian” geology”<sup>1</sup>

Yet, in law we find ourselves asking about the different approaches that national laws take in respect of the overwhelming majority of legal areas. For us, in law there is such thing as English law, American law, Japanese law and so on. This tradition of ‘national’ laws goes back to the tradition of the Nation State, as this was given birth in 1648 through the Treaty of Westphalia. For better or worse, States have chosen to create their ‘own’ laws (even if one has it in good authority that laws tended to be transfers or borrowings from one part of the world to

---

1. Zweigert & Kötz, *An Introduction to Comparative Law* (Tony Weir, 3<sup>rd</sup> ed. Clarendon Press, 1998) 15.

another) so that they uphold their *imperium* (legal power) over their *territorium* (territory).

Law was and still is a symbol of national unity. All in all, the situation we found ourselves in the discipline of law is one of overall divergence of legal system to legal system. Exceptions here are the islands of legal unity between otherwise different legal systems through the relevant regulatory tools from such international organisations as the Council of Europe, the European Union, the World Trade Organization and the United Nations. Those examples are not without criticism, especially when it comes to their slow reflexes, their bureaucratic structures and their frequent distancing from their 'clientele' whether in the form of States or citizens. I would be the first to accuse their bureaucratic character; yet, the purpose of this analysis is not to demolish but to build on current matter. And whilst these organisations are in one way or another conservative and inward-oriented structures, worthy of reform to a greater or lesser extent, these organisations need to be supported, especially when they promote what we in law would call the legal convergence thesis. Additionally, together with the promotion of the idea of convergence of legal systems through such organisations, the very discipline of law is also promoted, through the very re-invigoration of the discipline by way of the mechanics and outcomes of such an approach.

At this initial stage of the analysis, however, it could be maintained that the convergence thesis is defined by a degree of beauty, a degree of ideology and a degree of essence. The beauty of this thesis can be found on the fact that the convergence thesis can be found on the principle of one-over-many or what we could loosely call the 'Platonic One', a defining idea of Plato's world-view. Plato reminds us:

'We are in the habit of positing a single Form for each plurality of things to which we give the same name'<sup>2</sup>

whilst application of the principle of one-over-many is found in Plato's definition of beauty:

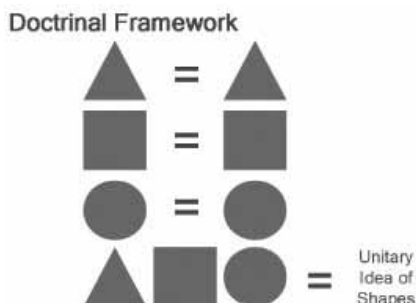
'... if there is anything beautiful besides Beauty itself, it is beautiful for no other reason than that it shares in that Beauty. ... nothing else makes it beautiful other than the presence of, or the sharing in, or however you may describe its relationship to that Beauty we mentioned, for I will not insist on the precise nature of the relationship, but that all things are made beautiful by Beauty'<sup>3</sup>.

---

2. Plato, *Republic* 596a (emphasis added).

3. Plato, *Phaedo Ph.* 100c-d (emphasis added).

This parallelism can apply to all aspects of human life (including legal systems). Thus, the following is true of our doctrine under the convergence thesis:



In accordance with the modern convergence thesis it is not the different shapes that matter but rather the fact that all shapes are shapes (see 'Doctrinal Framework' diagram above). By extension it is not whether different legal systems come up with different solutions in the face of e-laws; it is whether or not those different legal systems have e-laws in the first instance and laws which can be assimilated by way of legal outcomes, despite divergences in application. It is not the different colours that matter; it is the fact that these are all colours. It is not the different shapes that matter; it is the fact that these are all shapes. Hence, it is not that different legal systems come up with different legal solutions; it is the fact that those 'different' solutions can be assimilated as a matter of a unified system of law, especially in areas which are non-culturally specific<sup>4</sup> such as eCommerce laws. Furthermore, there is essence in the modern legal convergence thesis: such essence arises of practicality and economic utility. Practicality emanates from the fact that single legal standards apply throughout. Economic utility emanates from the fact that there, the need for separate differentiated legislation is dispensed with so are the costs associated to such legislation. Finally, when it comes to the degree of ideology, one would be able to detect such ideology on the fact that our lives are governed by principle; so too the convergence thesis in one way or another governs, as a matter of leading doctrinal principle, much of the modern discipline of law.

What about the real then? Where would one find convergence of legal principle? Classic examples are the following in every modern legal analysis:

4. Platsas A.E., The Functional and the Dysfunctional in the Comparative Method of Law: Some Critical Remarks (2008) 12(3) EJCL <<http://www.ejcl.org/123/art123-3.pdf>> accessed 1 October 2011.

- The legal circle of 27 Member States participating in the European Union's integration initiatives
- The legal circle made out of 47 'Jewels' in the Crown of European Convention on Human Rights (ECHR)
- The legal circle of 76 signatory States to the UN Convention on Contracts for the International Sale of Goods (CISG)

What about the principles that drive convergence? Very briefly the following can be taken to be some of the leading principles that drive the modern convergence thesis:

- Principle of Fidelity
- Principle of Conferred Powers
- Principle of Subsidiarity
- Principle of Proportionality
- Principle of Conditionality<sup>5</sup>

The first principle (fidelity) asks from nation-states to refrain from breaching their international obligations; equally, the extra-national should not intervene in matters of national law, unless it has been conferred the relevant legal powers and authority to do so.<sup>6</sup> With regard to the classic principle of subsidiarity, this principle suggests that what can be achieved at the lower level of authority in a circle of convergence (national level) does not have to be the subject matter of legal interference at the higher level of authority (extra-national level) in the same circle.<sup>7</sup> Proportionality, on the other hand, requires the extra-national to exercise its administration in a fashion that does not go beyond *vires*, legal expectations and the very requisites of proportionality itself, i.e. the acts of the extra-national have to be suitable, necessary and proportionate *per se*. With regard to what the I perceive as another principle of the modern convergence thesis, the principle of conditionality. I would simply wish to suggest that this is a principle which deals with the imposition of conditions on the part of the extra-national to the national. There is an assessor and an assessed. The extra-national is normally the assessor, the national being the assessed. The national is asked to implement an

---

5. Platsas A.E., *International Economic Law and the Idea of Legal Convergence* (2009) 2(4) *IJPL* 383, 392.

6. Chalmers *et al.*, *European Union Law* (CUP 2006) 193.

7. A classic illustration of this principle can be found in Article 5 EC Treaty.



extra-national relevant agenda of convergent economic law in exchange for economic benefit.<sup>8</sup>

### **Paradox of Internet's Global Reach but Relevant Regulation's Local Reach**

One is at odds, however, when it comes to the very global nature of the internet and the parallel local application of various laws in the matter (mostly at the domestic and regional level). 'Cyberspace is global'<sup>9</sup>; cyberspace regulation is not. The sustainability of this paradox to this day is one that puzzles. In a world that unites in law, the diversification of e-laws is striking, if not alarming. How could it be that transactions or exchange of information at the global level be regulated at the local or regional level (mostly)? A cynic would respond: 'systems will not actually collapse in the absence of a global framework for the otherwise global system of the internet'. And yet, one cannot escape the question of desirability. After all, it is the responsibility of the law academic to maintain and uphold what is desirable (and realisable) as opposed to merely describing what the current *status quo* in the area is. One needs to ask whether it is more desirable to regulate the internet at the local level or at a more global level.

Surely, one would opine that regulating the internet at a global level would come with a number of risks. This is true, when one deals, with what the author understands as domestic-oriented areas of law (areas touching upon e.g. criminal law matters, family law matters and child law matters). However, this thesis does not hold validity, when it comes to areas of law that are not as domestic-oriented (eCommerce or even data-protection). In the former case, believe that local regulation can play a certain significant role. In the latter case believe that extra-national/international regulation should play a much more active role than it currently does.

Also, particularly striking is the fact that the internet as a whole is one of the clearest examples of globalisation. In particular, one speaks here of globalisation of information. However, the current legal regimes observed do not point to such finding. This is peculiar at the very least. National legislators (for better or for worse) have chosen to intervene in the matter. They did so on a piecemeal basis. Accordingly, law of global application has been caught between nation-centred politics and economics.

---

8. In this respect see the World Bank's approach; *Review of World Bank Conditionality* (World Bank 2005) 20.

9. Nederveen Pieterse, 'Global Multiculture: Cultures, Transnational Culture, Deep Culture' 1. <[http://www.jannederveenpieterse.com/pdf/Global\\_multi.pdf](http://www.jannederveenpieterse.com/pdf/Global_multi.pdf)>, accessed 30 June 2011.

Additionally, we should consider whether or not the internet should be regulated, if at all.<sup>10</sup> Here those who argue against regulation of the internet as a whole, are of the view that the internet and electronic information should be left to its own devices. I think whilst there is beauty in self-regulation, indeed self-regulation of cyberspace law, there should be ideally a minimum level of regulation in the area. That minimum level of regulation should be the case in the core area of eCommerce law in that eCommerce seems to be playing a powerful role in trade itself nowadays. Furthermore, there is also the view that existent law can be stretched to cover the sphere of internet matters.<sup>11</sup> Interesting as this approach may be, we have now reached the stage where sustaining such an approach would be perceived as inappropriate, if not naïve. Naturally, the complexity of internet applications currently is far higher than the equivalent of such applications ten years ago. In other words, the question will always have to be not whether or not domestic regulation can be stretched to cover these new fields of legal operation but what kind of new legislative solutions would be added to the ones existent in the traditional areas of law. So too, the question will always have to be how does the legislator (at the national, regional and most importantly at the international level) will not adopt reactionary approaches but pro-active strategies.

### **A World Orderly Chaos of Electronic Regulation**

This brings us to our next point: the nature of the beast, the beast's name being what we generically call the internet. The internet is generally a wild creature of its own which could live in principle without regulation. In addition, it has been rightly suggested that the internet is now owned by anyone.<sup>12</sup> Yet regulation there is; only that one would be able to argue that a close to a chaotic situation in global legal terms actually occurs at the moment. To put it bluntly: the internet in certain parts of the world is regulated, whilst in other parts of the world is little regulated or not regulated at all. So too, in the parts where the internet is regulated the situation resembles the Tower of Babel.

Naturally, the legal response that one might receive in relation to the regulation of the internet worldwide arises by way of an argument that provides that the internet 'reflects the human mind and society [in which case] we cannot avoid concepts of public morality and policy.'<sup>13</sup> Whilst the argument has a degree of validity in that all law reflects the social in one way or another, this argument

---

10. Lim Y.F., *Cyberspace Law: Commentaries and Materials* (OUP 2007).

11. Lim Y.F., *Cyberspace Law: Commentaries and Materials* (OUP 2007).

12. Lim Y.F., *Cyberspace Law: Commentaries and Materials* (OUP 2007).

13. Forder J. and Svantesson D., *Internet and E-Commerce Law* (OUP 2007).

does not seem to fully address the question of whether or not a global platform of communications can 'afford' local variation in its fundamentals. Somehow, the argument of policy considerations does not seem to hold firm ground with the author, especially if we orientate our analysis around eCommerce law. To make matters worse, where domestic regulation exists, the law hardly keeps up with developments in the area.<sup>14</sup>

In essence, we wish to question the diversification of electronic laws around the world, indeed the diversification of eCommerce laws. Such a divergence of legal matter in the rather straight-forward area of international commerce should alert us. Perhaps this may be the result of the very parochial but certainly beautiful nature of our subject, the subject of law. Or, a pessimist might argue, economic nationalism keeps regulation of the internet at the national level. Whichever the cause, the fact of world orderly chaos of electronic remains.

At best, we tend to have a national/regional approach followed in legal matters in the area of e-law. In the United States and Australia we see respectively instruments such as the US Uniform Electronic Transactions Act 1999 and the Australian Electronic Communications Act 1999. Whilst those instruments would facilitate e-transactions in the domestic spheres of the United States and Australia adopting legal ideology from the UNCITRAL Model Law 1996, these developments remain exclusively domestic, i.e. have limited effect upon the jurisdictional sphere of the respective systems only. Equally, the Electronic Commerce (EC Directive) Regulations 2002 is regional and applies to consumers only. The effect of further forthcoming legislation of the EU in the area remains to be seen. Beyond these national and regional developments, I wish to bring to the notice of the reader that the failure of e-laws has been more remarkable where those laws are actually needed the most: in the international sphere. Whilst the term 'failure' would not probably be the politically correct one, we could not call these international eCommerce law projects a success either. In fact calling those projects a success would exaggerate the point when it comes to the limited remit of these projects.

We will not examine here what the reasons of their little success have been. That would be a pointless exercise in the sense that most such projects fail for lack of political will, which would otherwise manifest itself through ratification and incorporation. In any case, we observe that, at the international level, the effect of the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures 1996 and 2001 respectively and the UN Convention on the Use of Electronic Communication in International Contracts 2005 have been less than successful. To this effect the facts speak for themselves: only 43 national legal systems/or-

---

14. Forder J. and Svantesson D., *Internet and E-Commerce Law* (OUP 2007) 5.

ders (out of a total of approximately 200 national jurisdictions in the world) have adopted legislation based on the 1996 Model Law;<sup>15</sup> the 2001 Model Law has been adopted by way of national legislation in 17 States (out of approximately 200 States),<sup>16</sup> whilst the 2005 Convention has been signed by 18 States (out of approximately 200 States), ratified by 2 out of those States which have signed it but was brought into effect by none.<sup>17</sup>

Regulation, when it comes to the internet, is probably something which goes against the very essence of freedom that comes with it. Nonetheless, a minimum degree of regulation is needed. Even more so one could argue that such a regulation is needed at the global level. If the internet is of worldwide remit, would it not make sense that legislation on a global scale regulates the internet? Should it not be the case that global issues related to the internet are dealt with in a global fashion? Conversely, a crucial distinction is to be made here. Before we address this distinction we would have to divide areas relating to the internet as culturally confined and non-culturally confined. The point has been raised above but is worthy of elaboration. To elaborate and crystallise our thesis here we need to refer to subject areas within what we call electronic law as a whole. For instance, information law, data-protection law and freedom of information as a whole as well as the right to internet access could all be perceived as areas which touch upon the legal mentality of a given legal system. Correspondingly, if this is the case these areas of e-law should probably be regulated on a domestic basis (unless, of course, a constellation of States would wish to agree otherwise in the area i.e. by setting out a legal agenda of common/convergent legal standards). On the other hand, an example of a non-culturally confined would clearly be commercial law (or eCommerce for the purposes of our analysis). There is little that could make commercial the exclusive cultural artefact of any legal mentality anywhere in the world. Von Savigny has reached this thesis sometime ago.<sup>18</sup>

I strongly affirm this position. If this position comes with a significant degree of validity, then the area of eCommerce (just like the generic area of commerce) is not one which would be confined to a given legal culture. This returns us back to our initial point: there are areas of which are not culturally influenced. Commer-

---

15. <[http://www.uncitral.org/uncitral/en/uncitral\\_texts/electronic\\_commerce/1996Model\\_status.html](http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html)> accessed 10 October 2011.

16. <[http://www.uncitral.org/uncitral/en/uncitral\\_texts/electronic\\_commerce/2001Model\\_status.html](http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_status.html)> accessed 10 October 2011.

17. <[http://www.uncitral.org/uncitral/en/uncitral\\_texts/electronic\\_commerce/2005Convention\\_status.html](http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html)> accessed 10 October 2011.

18. Halley J. and Rittich K., 'Critical Directions in Comparative Family Law: Genealogies and Contemporary Studies of Family Law Exceptionalism' [2010] 58(4) *AJCL* 753, 771.

cial law, in its traditional sense, is one of them. By extension, if global regulation would arise in the sphere of eCommerce, then one could readily claim that little would change in the core cultural element of national legal systems. Thus, it is only natural that eCommerce qualifies as one of the areas of e-law that can be a major field of convergent (if not uniform) legal standards around the world.

### Unified Legal Standards as the Way Forward in eCommerce

Concentrating then on the key area of eCommerce in the sphere of internet law, one understands the matter as of one of key priority when it comes to the creation of unified electronic standards. There are many reasons for this but they all lead to one overall reason: *practicality*. Rather than having lawyers arguing on private international law rules, it would be significantly better for traders and consumers, if uniform or close to uniform standards of legal application were *ab initio* the case. Those could apply anywhere on the basis that we would have a circle of legal systems which would comply with the same standards of eCommerce. Thus, plaintiff from State A would be able to seek compensation against defendant from State B in jurisdiction Z, A, B and Z being States which would all be compliant with the same legal standards. It would not matter where the case would be heard, as there would be mutual recognition of awards irrespective of whether the case would be heard in jurisdiction A, B or Z.

Goldman has argued elsewhere that '[t]echnology is a key element of globalisation'<sup>19</sup>. Again, the question that we need to address is how do national standards fit in the otherwise international phenomenon of technological development? How does eCommerce make itself compatible to the fact that it is nationally-regulated when it is –by definition– an international phenomenon? One response, that of traditional private international law, is that which provides that all these matters can simply be regulated by choice of law clauses. Let us call this the 'freedom of contract doctrine approach'. Another approach, close to that of private international law, is that which suggests that we should not be concerned with such issues (even in the era of the information society), the reason being that such matters are matters falling within the sphere of national sovereignty. Let us call this the 'national sovereignty approach'.

Finally, last but not least, there is (or at the very least there should be) a third approach, the 'convergence of systems in legal matters' approach. The analysis on the above points to the following: first of all, the 'freedom of contract' approach, irrespective of its attractive character, does not give us an answer as to how inter-

---

19. Goldman D.B., *Globalisation and the Western Legal Tradition: Recurring Patterns of Law and Authority* (Cambridge University Press 2007) 25.

national matters are regulated in an international fashion. Second, the 'national sovereignty' approach is one that comes from the sphere of public law. This point is crucial for our analysis: traders, indeed e-traders, would not be particularly interested to engage with the *territorium* and the *imperium* of States in international eCommerce matters in the sense that these questions do not directly inform international trade practice. Surely, to this day, international trade matters (save in the cases of a neutral third party adjudicator) are normally dealt at the national level of litigation but that alone does not promote our analysis, in the sense that this is a mere depiction of the current *status quo*. Third, by comparison to the two approaches already explained above, it is opined that the 'legal convergence approach' presents a considerably advantageous approach in that it dispenses with the need to private international law rules. So too, national sovereignty plays an insignificant role here in that such approach (that of national sovereignty) has little to offer to traders in the sphere of international eCommerce.

It is projected that by the year 2013 the world eCommerce market will be in the region of \$1 trillion. Considering the high volume of transactions taking place electronically these days, one queries the reluctance of legal systems around the world to reach a common core of legal principles in the area. After all, this would be an exercise of practicality and enhanced economic utility.

## Conclusion

The developments on the internet proceed at a much faster pace than corresponding developments in law. It is crucial that a minimalist type of regulatory regimes, at a global level, is agreed, especially in response to the needs of areas which would not be otherwise culturally confined to the national. The need for global regulation becomes ever-increasing, especially because the relevant regulatory moves are currently confined to the national and regional level mostly and because there is now a particularly high degree of interconnectedness of world economics. Considering the great need for such worldwide convergent regulation, one is at odds with the languish reflexes of law and politics in the area. At the very least, the central, but otherwise non-culturally specific area of eCommerce law, can be an area where the various national/regional e-laws come closer. It is believed that this will benefit not only our world traders but also our cosmopolitan consumer. Trade sees no barriers. For this reason both traders and consumers would wish to be treated in pretty much the same way whether they would deal in their home jurisdiction or abroad. If this is to be achieved, it is hoped that political will on the part of the relevant political forces and affected States will drive the agenda towards considerable re-alignment of the national to the extra-national in the area. Otherwise, it would be only regrettable that most of our current legislation in the area is of regional success at best

# **European public sphere and digital political communication: Facebook as a medium of political expression and participation**

---

---

**Helen Rethimiotaki**

---

---

## **Introduction**

The notion of European public sphere emerged in the mid-1990's within the context of the public German debate regarding European Constitution. The question was how to reinforce democratic deliberation about E.U.'s political and legal process albeit the lack of common media, common language and shared identity. The European Constitution gave the opportunity to develop a transnational debate which led to a larger discussion about the political "nature" and dynamic of E.U. Since the process of European Constitution's sanction has been interrupted the discussion focused at the need to engage European citizens more actively in the discussion of European affairs and in the decision-making process. What are the prospects of emergence of a European public sphere in reality? Should the efforts aim at strengthening the channels of representative democracy or also promote "alternative" versions e.g. a more participatory or direct democracy?

Of course the effort to enhance political communication between European institutions, political parties and European citizens includes the use of digital communication technologies. Certainly its use has considerable advantages. Moreover, in the European level the use of interactive Internet as a medium of political communication is especially promising because of its inherent transnational character. However, critical approaches proliferate putting into question the potential of digital communication technologies due to some equally serious disadvantages. Do findings of social sciences help to identify and evaluate the use of digital technology in order to politically communicate and to enhance participation at the European institutional level? Could they actually create a virtual European public sphere?

This kind of theoretical approach is also valid for the use of interactive Internet e.g. Facebook and blogs as a remedy to the crisis of national representational European democracies and E.U.'s deliberative deficit. Although in the beginning many expected that especially Web.02 would provoke a revolutionary change in political communication, in reality technology can not by itself subvert the structural conditions within which it functions. However, this does not mean that in-

teractive digital technology is not politically significant as already shown in cases where Facebook was used as a medium of political opposition or activism. Regarding European public sphere what are the (still) limited empirical data of its use and to which (still) provisional conclusions they lead? What are the questions that need to be further examined?

From a legal point of view political rights of European citizens must be protected also when they exercise them by using digital technology. This can be the case when they use Web2.0 to get political information from European institutions, to come in contact with political parties or candidates, to express political opinion, to produce political news or even to organize political activism. Respectively European law sets limits e.g. European anti-terrorism legislation which can complete or compete national legislation. From a point of sociology of law it is being asked whether private space invades the public one or whether they merge by slowly eroding the legal categories concerning political participation.

Under the above mentioned theoretical perspective this article will try to answer the following questions:

1. What does the notion of "European public sphere" describe, which components includes and what is its explanatory value after the failed 2005 Constitution attempt?
2. What is the potential of digital communication to intensify political communication and to broaden political participation at the European public sphere?
3. Can Facebook and blogs go beyond private communication, become a medium of political expression and enable a more direct democracy?
4. In this case what are the political rights to be preserved and the legal limits to be set? Could the relevant legal categories be affected and in which way?

## **1. European public sphere and its critics: stagnation and prospects after European Constitution**

The notion of "public sphere" was reintroduced by German philosopher J. Habermas during 1960 in order to describe the symbolic arena of political discussion and public reasoning that originated from the cultural institutions of the early 18<sup>th</sup> century bourgeoisie. This cultural sphere mediated the tension between centralized political power and political groups. From mid-1990's the concept is used with reference to E.U. and largely redefined. Essentially the European public sphere has been defined in two different ways (Meyer, 2008): First as an arena of discussion of European affairs according a liberal conception where mass media have a key role. It refers mainly to the process through which European citizens form an opinion and indirectly provide feedback to European institutions



or control them. Secondly as a transnational structure of communication, a network of information and opinion exchange among citizens, media actors and social groups regarding matters of European politics. Whereas the first refers mostly to a vertical kind of link of European citizens to European system of making political decisions, the second fosters an horizontal one because it tends to normatively appreciate transaction among citizens. The second one reflects better the discursive understanding of public sphere that is “a network that gives citizens of all member states an equal opportunity to take part and encompassing process of focused political communication” (Habermas, 2001). So according an extended notion which includes both vertical and horizontal dimensions European public sphere components are the following (Bee/Bozzini, 2010):

- a. *European institutions*: they diffuse their positions, openly debate about them and answer the citizens’ questions accepting their feedback.
- b. *European and national political parties*: they deplore and synthesize the political dimensions of European policy choices and the consequences of these choices.
- c. *Mass media*: they systematically refer to European issues in order to make visible European actors, issues and policies and the European aspect of national issues
- d. *Civil society associations* (e.g. private companies and NGOs) *and groups of citizens*: they diffuse their problem definitions and propose solutions, amplify the relevant debate and express contestation.

Ideally a European public sphere would emerge if European issues would be intensively discussed simultaneously in all European countries. This requires a discussion of the same themes with similar frames of reference, of the views of actors of other European countries and of the positions held by European institutions and non-government actors (Meyer, 2008). Such maximal vision was of course criticized with the argument that it is conceived as a replication of public national sphere although the political conditions of E.U. differ profoundly. First the political subject that the public discussion is referred to can’t be clearly identified. Political power in E.U. is diffused, the European system of decision making is not visible enough and the chances for citizens’ participation are vague. Secondly there is a great linguistic and cultural heterogeneity among European citizens. To what degree is a European “we” constructed and how does it relate to national “we” (Eriksen, 2005)? Any communicative community presupposes a certain degree of unification through shared culture and identity. And even this may not be enough in the case of E.U. because democratic deliberation aims to define the collective good for a political community (Steeg, 2010).

These are serious arguments that can’t be easily by passed on but within the limits of the present article we would like to focus specifically at the impact of the

failed European Constitution to a likely emergence of a European public sphere. Has European Constitution been an issue publically debated at the same time in all members States? Did it provoke a transnational public debate proving the mutual acknowledgement and observation of each other in a common context, using the same criteria of relevance? The mere failure of the project proves that it has not been such a case. However, the failure of the European Constitution had definitively an important impact in the emergence of European public sphere. From one point of view it officially declared the end of the permissive consensus to the political project of European unification. Administrative elite and legal scholars took for granted that European citizens would once again consent to their projects by showing their indifference. But during last decade European integration process has become an increasingly controversial one. E.U. gradually became an object of an intense political antagonism between national political parties. National media comment systematically on European affairs. They made them visible but at the same time they contested E.U.'s developmental efficiency combined with re-distributional, social problems it creates.

Finally recent social research shows a growing negative public opinion about Europeanization mostly related to national identity problems (Hooghe & Marks, 2009). From another point of view although the failure showed that E.U.'s democratic deficit could no longer be ignored. It has proved how deeply the discursive disempowerment of civil society is embedded in the Europeanization process (Statham, 2010). The legal innovation of a Constitution not only without a State but also without (a) people(s) could not reduce the democratic deficit by enhancing citizen's rights of being politically informed, of expressing political opinions and of participating in the political process of European unification. The gap between intergovernmental agreements and civil society has never looked bigger. EU's consultation processes remained strongly top-down and reserved to insiders, whereas civil society remained completely out of the debate (Statham, 2010). The Europeanized public debates are less inclusive of civil society than national ones.

In conclusion the extended meta-theoretical concept of European public stands between an empirically meaningful concept and a normative expectation expressing a fundamental democratic prerequisite. At the present, Europe has acquired visibility. Since the public has shown its self not to be uni-dimensionally in favor of European integration, mass media became an important actor within European public sphere who also criticize European decisions and projects. The bottom-up mobilization of civil society remains a prospective project since there is no doubt that European citizens have to get information in order to form an opinion and be involved in the relevant argumentation. Only then they would be enabled to express their consent or dissent at European decisions. The project is also linked

to the debate regarding the democratic basis of European political system and the search of new forms of citizens' inclusion. Lisbon Treaty combines the efforts to enhance the traditional forms of representation through the empowerment of national parliaments with new forms of participation, based to deliberative and associative democracy. The potential contribution of digital communication technologies of new generation, the interactive Internet and its chances to allow direct political expression of civil society bottom up is of great interest.

## **2. The potential of digital communication to broaden European political communication, contestation and participation**

Since the mid-90's when European Union as a form of transnational governance was confronted with the (pseudo)dilemma to choose between efficiency and democracy the power balance of its institutions has been improved. Undeniably there has been done a lot of things to enhance democracy, but it seems that the problem of transnational governance is inherent; it inclines to the empowerment of the already powerful executive actors because of strong barriers to the development of civil society and processes of democratic deliberation (Statham, 2010). One thing that complicates the effort of democratizing E.U. is the vagueness of the target to achieve. At the moment the national model of collective representation undergoes a legitimacy crisis after the end of neo-corporatism, where efficiency was combined with participation of limited organizations in policy making process (Saurugger, 2004). The simple replication of the modern democratic ideal and its abnormalities at a European level is neither desirable nor possible because of the way E.U. decision making system has been constructed. There are also two alternative models of democracy mostly discussed during the last fifteen years, the deliberative and the associative models. The deliberative one is concentrated at the process of public dialogue and at setting its forums. The associative one is interested in the institutional framework allowing civil society to participate in policy-making procedures (Saurugger, 2004). However promising they may be, they are not so easily adaptable to the present institutional framework. In the mean time, the degree of political apathy and passive consensus is raising.

Digital communication, especially Web.2.0, was visualized as a polyvalent remedy against the ever fainting interest of citizens to get politically involved at national level. At European level the prospects are more dynamic because of the necessarily transnational character of political communication about European affairs and the distance of European institutions from national audiences. Generally, many communication theorists estimate that communication technology has a great capacity to revolutionize the process of political interaction and even equalize the balance of power (Papacharissi, 2010<sup>1</sup>). There is a number of argu-

ments for the subversive power of technology, especially the interactive Internet, used as a medium of political communication. Some of them apply also or even more at European level. However, this does not mean that the latest generation of information and communication technologies can neither reshape national democracies nor create by itself a European public sphere, provoking at long term a real shift of power at European level. If and how it can promote political communication when used as its medium and whether it can actually become a medium of participation in the European public sphere still remains an open question. In the mean time let us consider its theoretical European prospects in relation with the mixed results that social research has come down to.

The positive contribution to the development of European transnational public sphere comes from four main advantages of ICTs, a technical, an economical, a political and a cultural one. First, it obviously disposes a considerable technological advantage because it enables a two-way communication, bottom down and bottom up. It can transmit informational outputs, but it can also receive inputs, especially questions which can further guide European institutions or political parties to stimulate political interaction. It can create an online environment in which European citizens can meet politicians of European political parties and discuss policy choices. The activity that involve e-participation and online debate increased the last years and the topics were amplified e.g. European Commission's website ([europa.eu.int/futurum](http://europa.eu.int/futurum)) regarding the institutional future of E.U. (ETAG, 2011).

Secondly, it disposes an economical advantage because it reduces the cost of information distribution and it makes the access to it less time consuming (Genaro & Dutton, 2006). This could bridge social inequalities and may allow to remote social groups to form complaints, proposals and petitions (e.g. [ec.europa.eu.yourvoice](http://ec.europa.eu.yourvoice)), thus changing the so far elite features of political participants. Thirdly as far as political communication about European affairs is concerned there is a political advantage for both national political system and European institutions of decision making. As nation-State's power is reduced and it's relation to economy is transformed there is a growing communicative tension between political parties and the spontaneous and unorganized civil society (Tsiros, 2007). In theory interactive Internet e.g. Facebook, webblogs, online newspapers and websites could create opportunities for a more direct kind of democracy. In this way issue-related transnational communities would be build up. As national public sphere becomes gradually de-territorialized (Winter, 2010), these episodic or social communities would diffuse values that eventually could constitute the core of a transnational identity and finally substantiate European citizenship (ETAG, 2011). Forth, following the most optimistic scenario the social networking media has a strong cultural advantage, since late modern fragmented

selves dispose a weak sense of belonging to a political community private, personal und unofficial easily mingles with public, common and institutional intervention. Citizens who can be several part of different cultures, at the same time, are more inclined to participate in a different kind of process without the direct intention to influence political decision (Dahlberg, 2007 & Tsiros, 2007).

However, social researches conclusions do not justify the great expectations invested in ITCs used as a medium communication. They offer a variety of counter arguments, which rather speak for a critical approach. First, generally digital technology is mostly used for commercial and leisure activity. Due to potential advertising benefits commercial interests run through the whole range of digital communication process. Anyhow its use for political purposes still remains in comparison marginal (ETAG, 2010). Secondly even in case of use for political communication, empirical data show that social inequalities usually observed at political participation are reproduced. Younger people with higher education and socioeconomic status, who are anyways advanced users of digital technology tend to use it also for getting political information (Genaro & Dutton, 2006). In addition the most politically active online are already actively participating in politics.

Especially regarding the European public sphere online participation, a highly specialized public is overrepresented which anyhow is actively involved in European affairs (ETAG, 2010). So diversity of participants is not automatically provoked by mere technology. Thirdly, online discourse is highly fragmented. In addition anonymity and possibility of shifting identities means lack of solid commitment (Karakaya, 2005). Rational critical debate differs from simple registration and flow of individual views. Multiple networks of connected citizens and activists can't be so easily transformed in united cultural collectivities. The experimental identity construction e.g. regarding specific issues such as the environment, can't overcome post modern political identity only because of the use of Internet technology (Kahn & Kellner, 2004). The reason is that the current structure of social networking platforms advance individualization and fragmentation, because they are centered at individual creativity and performance-driven and competitive effort (Fuchs, 2009). Forth the ability of self producing information does not create per se a virtual European public sphere, because participation means to gain a degree of control over decisions. Information must also become visible, attract the attention of decision makers and finally influence their decisions (Fuchs, 2009). This can happen only if the political system is firmly committed to a more citizen centric function (Coleman & Blumler, 2009).

In conclusion, it seems advisable to avoid theoretical extremities and continue empirical research especially because European public sphere has recently start-

ed to develop. Digital political communication can neither subvert the structural conditions of political communication for European affairs and the conditions of participation to the political process of building E.U. Nor it can replace the traditional political communicators who institutionally retain the full capacity of defining shared problems and their solutions despite the legitimacy crisis they undergo. Concepts about using digital technology to enhance political participation have to incorporate theoretical conclusions about it. ITCs can actually be integrated into traditional offline forms of participation not a substitute to them. However, if political decisions are met to use digital technology as a medium of enhancing democracy at European level it has great potentials. It can facilitate the effort of European institutional and political actors to link back participation to representation. It can also connect transnational publics around specific issues, despite the cultural differences of European political audiences. Finally it can express strong political contestation and provoke a re-evaluation of decisions in both national and European level. These theoretical prerequisites are also valid for the use of Facebook and blogs. Here the main question is whether they can facilitate a bottom up political expression and, furthermore, if they can contribute to structure a transnational European public sphere.

### **3. Facebook & blogs: could they enable a more direct democracy?**

In mid 2000, after the record abstention in the European elections of 2004 there has been a paradigmatic shift of European political communication strategy (Aldrin & Utard, 2008). Instead of simply diffusing information to specialized agents and audiences and collecting data through opinion surveys, European institutions have set as target to elaborate a communication policy through participatory debates. The White Paper on European Communication Policy (COM 2006, 35) followed a serie of debates referred to as Plan-D for Democracy, Dialogue and Debate (COM 2005, 494). The paper aimed at mobilizing all the key actors (EU institutions and bodies, the Member States, regional and local authorities, political parties and civil society) to do four things. First to define common principles for communication on European issues, second to empower European citizens, third to work with the media and new technologies, and forth to understand public opinion. Regarding ITC's European institutions and actors should take advantage of Internet as a political communicator aiming especially at strengthening European democratic function with participatory elements.

New media can theoretically give direct voice at a trans-European public sphere in contrast with traditional media which represent citizens at the national one. They can stimulate citizens to communicate with their representatives, to confront them and to directly express their opinion about European affairs in di-

dialogue forums. Despite the ambivalences of the project to politicize European communication (Aldrin & Utard, 2008), the recent evaluation of political communication by personal media regarding within E.U. shows that there has been a considerable increase of their use (ETAG, 2010). Inspired by President's Obama campaign, European political parties have, more or less, incorporated interactive Internet in their effort to communicate with national political audiences on European affairs. They have tried to establish communication especially with young audience to which they have previous difficulties to get connected. But there is a crucial question raised; beyond updating methods of political communication by transposing participatory marketing technologies, in reality can personal media function as a virtual European public sphere as the rhetoric of the White Paper on European Communication Policy urges? Do they contribute to a public opinion formation about E.U.? Do they really stimulate political expression of consent or contestation? Do they enhance citizens participation by enabling them to make their own public news and redefine the political agenda? What does empirical evidence suggest? Before referring to it, we should formulate the proper theoretical questions in order to considerate it and come down to reasoned, at least provisional conclusions.

National public sphere is held together as a common normative horizon by the unifying force of print media and television who speak in front of their public about shared problems and their solutions (Trenz, 2009). Beyond the normative self-description of the digital public sphere as a cosmopolitan, here "pan-European" releasing virtual public from national bonds what does communication by interactive Internet represents? Do citizens who communicate within their private sphere, individually or in groups develop shared understandings of self-government claiming to be politically expressed? Under this perspective it must be examined if Facebook and blogging etc restructure public sphere, if they tend more to stimulate, engage and integrate rather than distract, disintegrate and fragment (Trenz, 2009).

To begin with empirical evidence as far as political communication is concerned there are already some, at least, indicative findings about the use of interactive Internet bottom down that is from European institutions, e.g. the European Commission or European Parliament or actors such as European political parties and their candidates. For instance, there has been a study regarding Facebook and blogging used by political parties during EP's elections 2009 in Bulgaria (Marcheva, 2010). It seems that it had an influence in increasing the proximity of E.U. institutions to the citizens and involve them to the elections process. But then again generally all new E.U. members are more motivated to be engaged with E.U. related political processes. This is because their national public tend to consider it as a chance to be included in the European communication process as equal

members, given their previous limited freedom of political expression and communication (Lauristin, 2007). The European Parliament carried out an effective campaign on YouTube, it has a Facebook and Twitter profile, several online chats with its members and some online debates about European issues. The number of its members who use it has doubled since 2009. There is already a considerable majority amongst them which estimate that social networks are effective in political communication but less effective than personal websites (Fleishman & Hillard, 2011). In addition, the survey verifies that users of social media also visit online version of newspapers and reading online E.U. focused media in a remarkably high percentage.

As far as political participation is concerned from the bottom up perspective research has only recently started but there are some indicative results. For example, there is evidence that the nascent French blogosphere has been used as a medium of political opposition and effort to influence policy decision in case of Constitution referendum in 2005. Blogs played an important role in mobilizing the French "No" campaign (Drezner & Farell, 2008). However, the analysis of material that individuals decide to place at the Web regarding E.U. (realized by search engines and webometrics methods) shows that still the average Internet user is being politically informed from the platforms of its favorite newspaper or television (Koopmans & Zimmerman, 2010). Institutional actors are the main sources of information in the Internet, whereas civil society actors and social movements as news producers are less visible than in quality newspapers. At the moment a combined research is running within RECON (Reconstituting Democracy in Europe) research program ([www.reconproject.eu](http://www.reconproject.eu)). The program includes investigating whether an E.U. online sphere emerges from below through examining relevant communications in Facebook and independent blogging formation of online communities through user commenting and social networking (Michailidou, 2010). It will also try to evaluate the informative value and quality of E.U. debates in comparison to the professional journalist websites (also considered as a vertical online sphere).

The above mentioned conclusions prove that until now the emerging European public is not restructured due to social media, since the dominant players remain dominant in the traditional sphere, exactly where their communicative activity is also legally protected (Trenz, 2008). Beyond oversimplifying dilemmas digital technologies are appropriated in ways shaped by the social conditions within they are immersed. The employment of interactive web bottom down in order to communicate with European citizens about European matters it may be used to make more appealing representative democracy in a consumerist model or to accelerate pluralism and inclusion to decision making process. The bottom up political expression may be controlled and, also, political protest action may be



restricted in the name of fascism and or terrorism. Or, on the contrary it may favor the expression of social groups and opinions outside the main stream by decentralizing control of communication process. Anyhow at the moment is far from fully developed.

The fact that bottom up participation in European public sphere remains thin is not a mere question of technology. This is concluded also from comparisons with national political sphere. In many European national political scenes interactive Internet appears to accelerate three already existing trends, that is single issue campaigns, new social movements and radical direct action protest (Wars & Gibson, 2009). One may think that difference is due to the language barrier and the fact that participation is stimulated the more local the reference point is. However, the full globalizing dynamic of Facebook and its rapid transforming from medium of private communication to medium of political expression and activism was recently shown in North Africa and Middle East countries. There commercial logic, boulevardisation and segmentation were at least from first sight overcome under the pressure of given political conditions, the changing balance of power between repressive regimes and resistance youth movements. After all, objective political conditions and political representations such as the vision of a political common future largely define perceptions of the public or private nature of virtual community constructed by Facebook and social media. Given the different political conditions Facebook developed its full capacity as a medium of political protest in Middle East and North Africa countries. Oppression from authoritarian regimes indeed promoted the formation of collective identity and the feeling of community belonging constructing linkage with friends and groups with like-minded objectives. There are, of course, many objections regarding the normative quality of the kind of linkage between the protesting groups. For example, what is so rapidly diffused are simple or simplistic messages at moments of political tension without specification of their sources and political identity. But there is no doubt that this is a kind of political expression which is legally protected or limited under certain legal conditions. The question is whether the dynamic development of interactive Internet, which has only just began, can fit in present legal categories

#### **4. Legal rights to be preserved and limits to be set by European law: are present legal categories affected by interactive Internet?**

At the above mentioned context social networking tools such as Facebook, Twitter and YouTube clearly had a decisive influence on the way people communicated with each other out of their state borders. At the same time, the reaction of authoritarian regimes has shown that legal rights of users, who privately ex-

pose themselves to a carefully built public space, can be seriously menaced. The scope of the risk that run users in purpose of politically communicating through new media has turned out to be considerable. Governmental reaction also proved that, although usually depicted as uncontrollable, digital communication technology can actually be controlled when strong political or economical interests are at stake. Facebook pages were hacked in order to deface users and find out what they were planning to organize (Meier, 2011). Using malicious codes that record login information, the regime has stolen their identity in order to lure other users to meet at specific places for protesting purposes and finally arrested them. Also, Facebook accounts of political movement participants were deactivated. Anonymity was after all proved impossible. From legal point of view the question raised is what kind of legal rights have the users of online social networks when they use them within a context of political communication. Since they are standing between private and public space should their right of privacy, as basis of autonomy of action and self definition, be adequately protected or their expectations of privacy are diminished because of user's self exposure at the Web (Piskopani, 2009)? Should the legal notion of privacy be transformed in order to readjust rights and obligations of European citizens who now stand in a twilight zone (Panagopoulou-Koutnatzi, 2010a)?

In case of European public sphere the question seems a tragic irony. If European citizens are finally aware of the need and the benefit to get involved in the political process of Europeanization in any way available, is it safe to use interactive Internet for this purpose? Would it not be ironical if the effort to get collectively self determined would lead to sacrifice another piece of right to self determinism? In addition in case of Facebook (and not only) the American lower standards of privacy protection of processing personal data mingles with the higher European ones. Privacy is defined according to social constructs that evolve with time through collective social experiences (Piskopani & Mitrou, 2009). In the moment such a transformation takes place due to the combination of many working together factors. Digital technology has long enough been represented as uncontrollable. Terroristic attacks have given the chance of legislative reduction of privacy protection. A youth culture of self identification though manipulation of signs and spaces became predominant (Lash & Urry, 2002). Such being the case to which direction should existing European law of personal data protection be interpreted or even change in order to raise the protection degree to the level of risk that Web 2.0 sets (Mitrou, 2010)?

The field of application of social networking services offered through Web 2.0 continuously expand. From fun and leisure activity they are being used for business and politics (Opinion of art.29 Data Protection Working Party, 2009). This expansion creates tensions between basic freedoms and communicative faculties,

diffusion and concentration of information taking specific form in every field of social action. Particularly political communication using Social Networks Sites (SNS) can affect freedom of political expression, informational privacy and to a lesser extend secrecy of communication.

As far as freedom of political expression within European public sphere is concerned, there is a general legal framework which assures the protection of users. The European charter of fundamental rights assures the right to respect of privacy (art. 7), the right to the protection of personal data concerning him or her (art.8), the freedom of expression and the freedom to receive and to impart information (art 11). Also according T.E.U. every citizen has the right to participate in the democratic life of E.U. (art. 10.3) and E.U. institutions are required to inform citizens and publicly exchange their views (art. 11 TEU). European union institutions also have to ensure public debate about European issues (arts 15 & 16 T.E.U.). Freedom of political expression is also protected by E.C.H.R. and national Constitutions. However, freedom of political expression is not absolute but it can be proportionally restricted under given circumstances and according a given legal process. For instance, should political expression through SNS be “censored” in case of hate speech, racism or extreme right propaganda or systematic defamation of politicians?

Online political propaganda by far right political groups in Europe was already restricted (Copsey, 2003) and protest campaign activities have been monitored (Pickeril, 2003). The level of tolerance of democratic threat vary in European countries. For example, according the German Constitution even political parties can be banned or dissolved if their existence threatens the democratic order (Mavrias, 2002<sup>2</sup>). The Greek Constitution allows the banning of hate speech only exceptionally when the consequence of freedom of speech become intolerable (Panagopoulou-Koutnatzi 2010b & Anthopoulos, 2000). E.U. framework decision on terrorism (2002) has also contributed to narrowing the limits of this tolerance, to relax data exchange requirements, tracking down persons via mobile telephone and monitoring all forms of electronic communication through search engines. Whatever limitations in the name of surveillance of crime should be tolerable insofar as strictly necessary, proportionate and accompanied with adequate and effective guarantees against abuse (E.U. Network of independent experts on fundamental rights, 2006).

As far as the right of informational privacy of users of SNS is concerned, the providers of Social Networking Sites process their personal data, which in this case can be considered sensitive to the extent that they reveal political opinions and beliefs. It seems that the provisions of the personal data Directive (95/46/EC) apply to the providers even if their headquarters are located out of European

space (Group 29, Opinion 5/2009). This means that users of SNS have the rights of access, correction and deletion of the political profile information. Providers are obliged to assure adequate level of security, to offer choices of privacy settings and to inform the subjects before transferring their personal data for further processing. Users may be considered as controllers, if they are making publicly accessible at a website personal data of a third person (Mitrou, 2010). Diffusing the sensitive data regarding political opinions, beliefs or actions does not fall probably under the household exemption. This is the case when users operate only in a purely personal sphere just contacting people within the sphere of personal life. Sensitive data may only be published on the Internet with the explicit consent from the data subject or if the data subject has made the data manifestly public himself (Group 29, Opinion 5/2009). The point is that users are being exposed without giving an informed consent in full meaning of term to the providers. Without even realizing how far can information “travel” users upload information available to an unpredictable audience for unlimited time (Mitrou, 2010). This does not necessarily mean that they cede their right to privacy, the right of being in control of one’s information once they put up their personal information. Although young generations have a different perception of privacy and they make publically available a considerable amount of personal information as long as this information is automatically processed becomes personal data whose owners should be protected.

Providers can “leak” personal data not only to advertisers, but also to public authority. Should state authorities have access to publicly accessible information at the SNS? If the user has opted for a closed profile or has chosen a pseudonym in anyway shouldn’t his secrecy be lifted for detecting serious crimes or incitation to terrorist acts? Also, for security and legal reasons, couldn’t be justifiable to store data and accounts for a defined period of time in order to help prevent malicious operations resulting from identity theft and other offences (Iglezakis, 2009)?

At the moment as far as privacy of communication of users of SNS is concerned the answer is not thoroughly clear. From one point of view SNS *per se* falls out of the scope of the definition of electronic communication services provided in article 2 letter c) of the Framework Directive (2002/21/EC) (Group 29, Opinion 5/2009). One may say that the secrecy of any kind of communication is protected provided that at least one of the two communicants has taken measures to protect confidentiality (both their identity and the content of their message) and the communication medium is appropriate by its “nature” to sustain privacy (Chrysogonos, 2002). If participants have chosen to politically communicate through SNS, then this could be the case only if the user has activated safeguarding privacy settings, has a pseudonym and he has opted for a closed profile (Opinion of Attorney of Athens High Civil Law 9/2009). However, according interpretation

of USA Supreme court jurisprudence (which diverges regarding the expectation of reasonable privacy) even in this case the user has already accepted company's broad policy statement which includes company's right of access to his data and right to transfer them to the Police leading to users identification (Piscopani, 2009). Anyway it would be wrong to generally conclude that users, who use SNS in order to communicate political opinions and organize political protest, are in any case deprived of fundamental right to the respect of secrecy of communication only because of what kind of medium SNS inherently "is" regardless the social use they have given to it.

Finally in case that Facebook and blogs are considered as mediums of political communication, there will be many legal questions to answer due to the fact of their ambivalent private-public nature. For instance, political parties or politicians can use personal information, political opinions and beliefs expressed at Facebook for their political advertisement which requires sensitive personal data processing. Their rights to politically communicate with European citizens should respect the basic rules of personal data processing at European and national level (Greek Personal Data Protection Authority, Directive 1/2010). But once again the crucial question is whether people who express political opinions at Facebook or blogs can realize how far the lightly given information can be used i.e. for communication to promote political ideas. The same kind of confusion may appear in many cases where the judge should ad hoc decide whether blogs cease to be private spaces of idea exchange and become fields of political news destined to publically inform. Then blogs are transformed from medium of communication to medium of news propagation. This could justify the proportionate implementation of legislation regarding the press i.e. the banning of publication of opinion polls or results of political surveys during a given period before elections (Papakonstantinou, 2009). At the moment Greek courts jurisprudence tend to consider that such implementation cannot take place, because blogs differ substantially from mass media (First Instance Court of Piraeus, 4980/2009). Blogs are considered as semi public spaces resulting from interactive communication.

## Conclusion

The political use of Facebook and blogs transformed social networks from means of private communication to means of political, thus, public communication. The change is connected with many factors which are not mere technological (Chadwick/ Howard, 2008). Many underestimate this change thinking that anyhow social networks are highly individualized forms of online expression. For them they can only contribute to a broader social narcissism in our highly fragmented and individualized society. Some others believe it is due to a broader cultural change, thus they represent a real challenge to our understanding of democracy

(Papacharissi, 2010 and Ingelhart/Welzel, 2005). If we set ourselves in the middle we must admit that although a great deal of academic discussion regarding deliberative argumentation as a means of democratization of European public sphere, more and more European citizens produce audiovisual or direct communication deviating from the ideal of textual deliberative discourse. Indeed it might be time for the political theory to reconsider the scope of the subject "political communication". This may also include to encompass the role of affective dimension in regulation of political everyday life (Giddens, 1999) beyond the classical borders of the political system. At the moment it seems that already national political culture is being transformed due to the combination of technological and broader cultural change (Vernardakis, 2008).

From a point of view of sociology of law, the new social use of communication technology within European public sphere may as well lead to extend or even subvert the given legal categories regarding political participation and communication. This is also because European Union's political figure is not identical with nation state. The present legal categories are connected to nation state and representative democracy. It is not sure whether they can also work with the new complex political framework. At the moment we know what E.U. is not, but we do not know what it is becoming. It has been extensively discussed whether the national representative democracy can be reproduced or should it be enhanced with participatory democracy or direct democracy, even at national level (Venizelos, 2008:348). For historical reasons there has been an identification between democratic principle and representative system both considered as characteristics of rule of law. Nowadays, the high rates of political abstention, the devaluation of political parties and the higher degree of political system's heteronomy urge for new ways of understanding the contents of democratic values. In addition the freedom of political expression and right to participate in democratic decision making at E.U. level is broader than participating in so far weak European political parties (Papadopoulou, 2003) and deeper than electing and be elected. The legal basis of this potentially enlarged political rights are European charter of fundamental rights, E.U. treaties, E.C.H.R. and national Constitutions. Especially at the present context of economical crisis the simple register of voting for European Parliament is far from enough to legitimize the E.U. political handlings. All versions of political expression and potential participation in the European public sphere may contribute to enlarge the degree of E.U. democratic control, if basic democratic rights are respected and limited in a democratic way.

## References

- Aldrin, Ph./Utard, J.-M. (2008), The ambivalent politicisation of European Communication, Genesis of the controversies and institutional frictions surrounding the 2006 White Paper, available at <<http://workingpapers.gspe.eu>>.
- Anthopoulos, Ch. (2000), Protection against racism and freedom of information, Athens, Papazissis (in Greek).
- Bee, Ch./Bozzini E. (2010), Mapping the European public sphere, intititons, media and public society, London, Ashgate.
- Chadwick/ Howard, P., (2008), Handbook of Internet politics, Routledge, New York.
- Chrysogonos, K. (2006), Individual and political rights, Nomiki Bibliothiki (In Greek).
- Coleman, St./Blumler, G. (2009), The Internet and democratic citizenship: theory, prectice and policy, Cambridge University Press, 2009.
- Copsey, N. (2003) Extremism on the net: the extreme right and the value of the Internet In Gibson, R. Nixon, P. Ward, S., (eds) (2003) *Political parties and the Internet: net gain?* London: Routledge.
- Dahlberg, L. (2007), The Internet deliberative democracy and power: radicalizing the Public Sphere, International Journal of Media and Cultural Politics, 3, 47-64.
- Drezner,D./Farrell,H. (2008), Introduction: a special issue of public choice, Public Choice, 134, 1-13.
- Eriksen, E. (2005), The emerging European public sphere, European Journal of Social Theory, 8, 341.
- ETAG (European Technology Assessment Group) (2010), E-Democracy in Europe – Prospects of Internet – based political participation, available at: <[http://www.isi.fraunhofer.de/STOA\\_e.Democracy-Deliverable2-final version\\_02-2011.pdf](http://www.isi.fraunhofer.de/STOA_e.Democracy-Deliverable2-final version_02-2011.pdf)>.
- EU Network of independent experts on fundamental rights, Commentary of the Charter of Fundamental rights of the EU, available at <[http:// infoportal.fra.europa.eu/2006](http://infoportal.fra.europa.eu/2006)>.
- Fleishman/Hillard International Communications (2011), 2<sup>nd</sup> European Parliament Digital Trends Survey, available at <<http://www.epdigitaltrends.eu/S2011/downloads-2011>>.

Fuchs, Ch. (2009), Information and Communication Technologies and society: a contribution to the critique of the political economy of the Internet, *European Journal of Communication*, 24/1, 69-87.

Gennaro, C./Dutton, W. (2006), The Internet and the Public: online and offline political participation in the United Kingdom, *Parliamentary Affairs*, 59, 299-313.

Giddens, A. (1999), Risk and responsibility, *Modern Law Review* 62(1), 1-10.

Greek Personal Data Protection Authority, Directive 1/2010 about processing of personal data for the purpose of political communication, available at <[http://www.dpa.gr/portal/page?\\_pageid=33,23367](http://www.dpa.gr/portal/page?_pageid=33,23367)>.

Group 29, Data Protection working party, Opinion 5/2009 on online social networking, available at <[http://ec.europa.eu/justice\\_home/fsj/privacy/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm)>.

Habermas, J. (2001), Why Europe needs a constitution?, *New Left Review*, 5, 5-27.

Hooghe, L./Marks, G., A postfunctionalist theory of european integration: from permissive consensus to constraining dissensus, *British Journal of Political Science*, 2009, 39, 1-23.

Iglezakis, I., Retention of personal data electronically processed after ECJ decision of 10.2.09, case C-301/2006, Armenopoulos, 8/2009, 1278 (in Greek).

Ingelhart, R./Welzel, Ch. (2005), *Modernization, cultural change, and democracy: the human development sequence*, Cambridge University Press.

Kahn, R. /Kellner, D. (2004), New media and internet activism: from the Battle of Seattle to blogging, *New Media and Society*, 6/1, 87.

Karakaya, P. (2005), The internet and political participation: exploring the explanatory links, *European Journal of Communication*, 20/4, 435-459.

Koopmans, R./Zimmermann A. (2010), Transnational political communication on the Internet: search engine results and hyperlink networks, in R. Koopmans/ P. Statham, *The making of European public sphere: media discourse and political contention*, Cambridge University Press.

Lash, S./Urry, J. (2002), *Economies of signs and space*, Sage Publications.

Lauristin, M. (2007), The European public sphere and the social imaginary of the 'New Europe' *European Journal of Communication* 22/4, 397-412.

Marcheva, M., The real political power of the Internet: Facebook, a possible new hub of European elections?, available at <<http://rc10.ipsa.org/public/M.Martha>>.



Mavrias, K. (2002), Constitutional law, Athens-Komotini, Ant.N.Sakkoulas.

Meier, P. (2011), The impact of the information revolution on protest frequency in repressive contexts, Doctoral Dissertation, Tufts University, available at <<http://www.irevolution.net/2011/02/10/facebook-for-repressive-regimes>>.

Meyer, J.-H., An emerging transnational network of communication on European affairs? The European public sphere at EC summits 1969-1991, paper presented for the 7<sup>th</sup> European Social Science History Conference, Lisbon, 2008, available at <[http://www.aei.pitt.edu/Meyer\\_2008\\_Network\\_of\\_Transnational\\_Communication\\_pdf](http://www.aei.pitt.edu/Meyer_2008_Network_of_Transnational_Communication_pdf)>.

Michailidou, A./Trenz, H.-J. (2010), Mediating European integration: online political communication in European Parliamentary election campaigns, Arena Center of European Studies, University of Oslo, available at <<http://www.sv.uio.no>>.

Mitrou, E. (2010), Privacy at Web 2.0, Law of Media and Communication, 3, 319-327 (in Greek).

Opinions of Advocate Supreme Court Opinion 9/2009 and 12/2009, Commentary of Tsollias, Law of Media and Communication, 3/2009, 389-400, (in Greek).

Panagopoulou-Koutnatzi, F. (2010a), Websites of social networks as national, European and international challenge of privacy protection, Sakkoulas, Athens-Thessaloniki (in Greek).

Panagopoulou-Koutnatzi, F. (2010b), About freedom of blogs, Sakkoulas, Athens-Thessaloniki (in Greek).

Papacharissi, Z., A. (2010), Democracy in a digital age, Cambridge Polity Press.

Papadopolou, L. (2003), European political parties: subjects of political unification or bureaucratic mechanisms. In D.Tsatsos/X. Kontiadis (dir), The future of political parties, Athens, 373-426.

Papakonstantinou E. (2009), Legal consideration of blogs: on the occasion of publishing the results of polls, Newspaper of Administrative law, 4, 460-466 (in Greek).

Pickeril, J. (2003), Cyberprotest: environmental activism online, Manchester University Press.

Piscopani, A.M. (2009), The protection of privacy of Facebook users, Law of Media and Communication, 3, 338-353 (in Greek).

Piskopani, A.M./Mitrou, L. (2009), Facebook: reconstructing communication and deconstructing privacy law? In Polymenakoy/Pouloudi/Pramatari (eds) 4<sup>th</sup>

Mediterranean Conference on Information Systems, Athens Greece September 2009.

Saurugger, S. (2004), Representative versus participatory democracy? France, Europe and civil society, paper presented at the ECPR Joint Session of Workshops, University of Uppsala, available at: <[www.essex.ac.uk/ecpr/events/jointsessions/saurugger.pdf](http://www.essex.ac.uk/ecpr/events/jointsessions/saurugger.pdf)>.

Statham, P. (2010), Europe's search for an attentive public: what prospects? UACES Conference, available at <<http://www.uaces.org/pdf/papers/1002/statham.pdf>>.

Steege Van De, M. (2010), Theoretical reflections on the public sphere in the European Union: a network of communication or a political community?, in Ch. Bee/ E. Bozzini, Mapping the European public sphere, Institutions, Media and Civil Society, University of Surrey, Ashgate.

Trenz, H.-J. (2009), Digital media and the return of the representative public sphere, digitising the public sphere, 16/1 available at <<http://www.javost-the-public.org/article/2009/1/3>>.

Tsiros, N. (2007), For sociology of political parties at late modernity, Thesis, 100, available <[http://www.theseis.com/index.php?option=com\\_content&task](http://www.theseis.com/index.php?option=com_content&task)>.

Venizelos, E. (2008), Towards a meta-representative democracy. The institutional conditions of a different politics, Athens, Polis.

Vernardakis, Ch., Blogs in Greece at 2008: political culture and new public space, Monthly Review, 47(112), 33-35.

Winter, R. (2010), Widerstand im Netz. Zur Herausbildung einer transnationalen Öffentlichkeit durch netzbasierte Kommunikation, Bielfeld.

Wars S./Gibson, R. (2009), European political organizations and the Internet, in A.Chadwick/ P.Howard, Handbook of Internet Politics, Routledge, 25-39.

# **On uploading and downloading copyrighted works: the potential legality of the users' interest in engaging in such acts - the case of EU and US paradigm**

---

---

**Vasiliki Samartzi**

---

---

## **1. The position of the end-user in the context of file-sharing**

### **1.1 Introduction**

This article examines the scope of the reproduction for private use copyright exception in the context of file-sharing. Private use should be differentiated from commercial conduct that takes place in private. According to the Court in the Napster case, an example of commercial conduct that can take place in private is the downloading and sharing of content. The Court said that the trading of music online was commercial in nature even though no money exchanged hands (*A&M Records, Inc. v. Napster, Inc.*, 2001). It has been suggested that the questions 'is private use noncommercial?' and 'can commercial use take place in private?' are two different questions (Creative Commons, 2009). It has also been pointed out that users consider less commercial the personal or private use than creators, and this difference may be a cause or effect of file-sharing in which 'no money changes hands' (Creative Commons, 2009). This article does not examine whether private use in the context of file-sharing networks is commercial or noncommercial but, instead, it simply examines the scope of application of the private use exception in the context of file-sharing networks. However, even though the commercial or not character of the use is not examined, the premise is that the act is not commercial, otherwise, the exception for private copying could not apply in the first place (Directive 2001/29 EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society).

Between September 2003 and June 2005, the Recording Industry Association of America (RIAA) sued thousands of individuals who allegedly traded copyright music files illegally using P2P file-sharing software programs (Rimmer, 2007; RIAA, 2005). The copyright holders alleged primary liability for copyright infringement that arises when a user without permission from the rightholder reproduces or distributes a copy of the protected work. Apart from the US, the International Federation of the Phonographic Industry (IFPI) has also co-ordinated

suits against individuals who uploaded copyrighted songs onto file-sharing networks and legal actions were brought in 18 different countries (IFPI, 2006).

In the context of file-sharing, two main acts can be identified. Firstly, the downloading of the work, which allows the user to retrieve the file made available by another user, and, second the making available of the work, which gives third parties the ability to access the work. The unauthorized downloading, which allows the creation of a copy, could infringe the exclusive reproduction right (*A&M Records, Inc. v. Napster, Inc.*, 2001), while the unauthorized act of making the file available could infringe the exclusive communication to the public right including the making available right (Institute for Information Law, University of Amsterdam, 2007). Thus, when a work is downloaded or made available for download without the consent of the right holder, there will be an infringement of intellectual property rights. If the answer to the question 'who should be sued' is the Internet user who performs the downloading, then it would be important to see whether copyright limitations could be applied in the user's interest (Bernault and Lebois, 2005). Moreover, if the supplier of the P2P software or the Internet Service Provider is to be sued by the rightholders alleging secondary liability for copyright infringement, then the application of a copyright exception is also important since the existence of infringement in the first place by the user is a precondition for a finding of secondary liability (Hays, 2006).

## ***1.2 Short description of the file-sharing technologies***

A report prepared by the Federal Trade Commission (FTC) identified as one of the differences between P2P file-sharing technologies and technologies that use central server or other pre-P2P models the default sharing of files in P2P models in contrast to manually sharing of files in previous models (FTC, 2005). Three broad categories of P2P file-sharing technology were identified by the FTC. First, there is the centralized model, e.g. the Napster model (FTC, 2005). Napster operated a centralized directory of files, which was located on a centralized server or set of servers to which user computers ("peers") could connect via an Internet connection. An individual user could download the Napster software, connect to the server and then send a query for a particular file she wanted to obtain. The server would respond with information indicating which other peers had the file and the user, who made the query could then request the file directly from the corresponding peer.

Second, there is the decentralized mode, where the P2P network exists without a central server or rigid hierarchy, e.g. Gnutella (FTC, 2005). Third, there is the hybrid model, which is a combination of centralized and decentralized topologies (FTC, 2005). For example, the FastTrack protocol uses a two-tiered system consisting of "super nodes" and ordinary nodes rather than a central server. Each

node consists of an individual user's computer. "Super nodes" essentially perform the directory role that the centralized server provided in the original Napster architecture. Using the file-sharing software, an ordinary node connects to a super node and sends a query for a file, and then the super node checks its index of files and sends the ordinary node a list of any matches. The user can then click on a match to establish a direct P2P connection and obtain the file from the selected peer (FTC, 2005).

Bit Torrent is a different example of a hybrid P2P protocol (FTC, 2005). BitTorrent has many unique characteristics that make it possible for users to create an independent, distributed P2P network with an Internet connection and basic computer knowledge. One peer has a particular file and acts as a "seed" node. The seed node then breaks the file into a number of pieces of equal size and distributes them to several other peers that are seeking to obtain the file; each peer receives one piece. Those other peers then exchange pieces with each other until each peer has obtained a full copy of the original file. Because the seed node sends only one copy of the file-in pieces, to the other peers-the "sharing" process is more efficient and requires less bandwidth than if the seed node had to send a full copy of the file to each of the other peers. Moreover, instead of searching other users' hard drives, a BitTorrent user must search for a website that has the so-called "torrent" file associated with the file the user ultimately wants to download. The "torrent" file contains information about the location of the computer with the "seed" node for a particular file, and the location of the server, known as a "tracker," that is currently coordinating the exchange of pieces of that file. Clicking on the "torrent" file allows a BitTorrent user to join this exchange process. As soon as the user downloads a piece of the desired file, BitTorrent automatically begins uploading that piece to other users who are looking for that file (FTC, 2005; Edstrom and Nillson, 2009).

Finally, there are the new one-click hosters like RapidShare. RapidShare is not operating any type of index or search engine that would make files stored on its servers publicly accessible. Instead, the users decide whether or not to publish a link to files they have uploaded. Actually, the entire file is uploaded with a single click on their webpage. The company then sends the user a download link that he can use and give to others to use to make available the work to third parties. Thus, one cannot retrieve the file without knowing the link. RapidShare allows their users to upload a file without prior registration. Downloaders have to click through to the hosting website to access the file. Paying members get access to the files they want right away, while all other users have to wait in line.

### ***1.3 The legal battles against individuals who trade copyrighted material - primary liability***

#### **1.3.1 Uploading**

Uploading of unauthorized works generally infringes the making available right. This right was formulated to cope with the particularities of digital transmissions. Digital interactive transmissions blur the borderline between copy-related economic rights and non-copy-related economic rights (Ficsor, 2006). Arguably, this occurs, firstly, because dissemination of protected material in interactive networks may take place with the application of technological measures which allow access and use only if certain conditions are met by the user (Ficsor, 2006). Thus, the actual extent of the use is not always determined at the moment of making available it a work and by the person who carries out the act of making available. It is the given member of the public, who may obtain access and who chooses whether the use will be deferred, that is by obtaining a more permanent instead of transient copy, or direct, such as on-line studying of a database, on-line watching of moving images, on-line listening to music (Ficsor, 2006). Secondly, this occurs because some hybrid forms of the making available of works emerge which do not respect the pre-established border between copy-related and non-copy-related rights. For example, a copy obtained through the transmission of electronic impulses and a protected material used on-line, even in real time, entails the making of temporary copies (Ficsor, 2006).

Given the particularities of interactive transmissions, the various countries disagreed on which of the copy-related rights/non-copy-related existing rights should cover such transmissions. Two major trends emerged, one trying to base the solution on the right of distribution, and the other preferring a kind of general communication to the public right (Ficsor, 2006). In the end, the 'umbrella solution' of making available to the public right was preferred by the Diplomatic Conference. The umbrella solution uses the term 'communication to the public' and the publication-related term 'making available' in order to cover every possibility, that is a given country's domestic laws provide for a distribution right, a publication right, or a communication to the public right (Art.8 WIPO Copyright Treaty 1996). For example, U.S. has chosen to use the distribution right (Ficsor, 2006). However, even though sufficient freedom was left to national legislation in respect of the legal characterization of the exclusive right, Ficsor notes that "the acceptability of the differing legal characterizations of acts depends on whether or not the obligations to grant a minimum level of protection, in respect of the acts concerned, are duly respected" 2006.

Interactive transmissions have also another particularity, namely the difficulty in identifying where making available takes place, an issue closely connected to the identity of the uploader. It could be argued that the making available takes place either where the uploader uploaded the work or where the server or the internet service provider is based or at the reception point. There are two main theories. The first theory states that the communication takes place at the point of the initial transmission (emission theory), while the second theory states that the act of communication covers the whole process of transmission and reception (communication theory). Legal scholars argue in favour of the communication theory in Internet context which embraces both initiation and reception (Reinbothe, J., and S von Lewinski, 2002; Ficsor, 2002). However, a recent UK case seems to accept the emission theory (*Football Dataco Ltd and others v Sportradar GmbH and another*, 2010).

In the US, copyright holders own the exclusive right to distribute copies of their works to the public under §106(3) of the Copyright Act. However, there is a fight over the scope of the distribution rights in the P2P context and the question arises whether copies must actually be created on other users' computers or whether it is enough that the defendant offer or make them available for download. This debate is closely connected to the debate on whether the US copyright law grants a making available right to copyright owners. In particular, the making available right has been defined by legal scholars as

“an exclusive right to make a work available, (i.e., to offer copies of it), over the Internet or a similar network to members of the public who can decide whether to access or copy it. Such a “making-available right” could be infringed by either a person posting a work on a web site or by someone “sharing” it with specially designed “piracy machines,” like the file-sharing programs Grokster, Morpheus, or KaZaA (Sydnor, 2009)”.

At the centre of the problem lies the proper interpretation of the terms ‘to distribute’, which defines the scope of the distribution right that replaced the publication right granted by every prior U.S. copyright act since 1790, and ‘to authorize’, that defines the scope of all exclusive rights, in 17 U.S.C. §106(3). 17 U.S.C. §106(3) provides that

“Subject to sections 107 through 122, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following: (...) (3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending (...)”.

The Copyright Act does not define the word ‘distribute.’ However, it defines the term ‘publication’ in 17 U.S.C. §101 as including

“the distribution of copies or phonorecords of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending. The offering to distribute copies or phonorecords to a group of persons for purposes of further distribution, public performance, or public display, constitutes publication”.

Moreover, it is said that “a public performance or display of a work does not of itself constitute publication”.

Even though the Copyright Act does not define distribution, according to one view, this term encompasses offers or making works available, regardless of whether copies are actually disseminated (*Hotaling v. Church of Jesus Christ of Latter-Day Saints*, 1997; *A&M Records, Inc. v. Napster, Inc.*, 2001). According to a second opinion, distribution requires actual dissemination (*Perfect 10 v. Amazon.com, Inc.*, 2007). According to another opinion, ‘distribution’ is equated with ‘publication’ and, thus, simply making available works does not infringe the distribution right since, according to the definition of publication given above, ‘publication’ requires “the offering to distribute (...) for the purposes of further distribution.” In other words, copies must be actually disseminated (and copies must actually be created on other users’ computers) (*Harper & Row, Publishers, Inc. v. Nation Enters.*, 1985). Arguably, obtaining works for further distribution is differentiated from obtaining them for personal use, and it would usually be difficult to show that one who makes recordings available to a P2P network can be aware of the way in which the copies of the works he shared will be obtained.

In this complex context, three district court cases decided recently that making copyrighted works available for possible download through P2P networks is by itself not enough to violate the distribution right. In the first case, *London-Sire Records, Inc. v. Doe 1*, the Court stated that merely listing music files as available for downloading on a P2P network did not itself infringe the distribution right and that actual distribution of the works was necessary. In the second case, *Elektra Entertainment Group*, the Court held that distribution has the same meaning as publication and in light of the statutory definition of publication, merely “making (copyrighted works) available” did not violate the distribution right. Instead, plaintiffs would have to prove that the defendant distributed copies of phonorecords to a group of persons “for purposes of further distribution”. Finally, in *Atlantic Recording Corp. v. Howell*, the Court agreed with

“the great weight of authority that §106(3) is not violated unless the defendant has actually distributed an unauthorized copy of the work to a member of the public. (...) Merely making an unauthorized copy of a copyrighted work available to the public does not violate a copyright holder’s exclusive right of distribution”.



A similar requirement of actual distribution of the work for the purposes of further distribution does not seem to exist in EU law. For example, in the *Pirate Bay* case, the prosecutor did have evidence of copying made by the plaintiffs of their own works, which showed that works were unlawfully communicated to the public, but the plaintiffs could not show evidence of downloading by users of the Pirate Bay (Edstrom and Nillson, 2009; Manner, Siniketo and Polland, 2009; Wistam and Andersson, 2009). The fact that no evidence of downloading by users of the Pirate Bay was obtained prevented the finding of unlawful reproduction and an infringement of the reproduction right, but allowed the finding of unlawful communication to the public and infringement of the making available right. Therefore, it could be assumed that the 'actual distribution' of a work to the public, which results in the creation of copies on other users' computers, is not a prerequisite for a finding of infringement of the making available right.

In the course of uploading there is also the possibility that the uploader will infringe the reproduction right by making a temporary copy. It has been suggested that given that the right of communication to the public (including making available) is specifically tailored to apply to acts of digital transmissions, it would make sense for it not to overlap with the right of reproduction (Institute for Information Law, University of Amsterdam, 2007). Towards this aim, it has been suggested to reduce the scope of the right of reproduction in line with a normative interpretation of the right in the context of which the purpose of the reproduction will be examined each time to determine whether the right holder's authorization is needed in order to make the reproduction (Institute for Information Law, University of Amsterdam, 2007). Generally, if both notions of 'reproduction' and 'make available' are not interpreted as technical and merely descriptive notions, but instead as normative (man-made) and purpose-oriented notions that are used to define and delimit existing proprietary rights, then the act of uploading will not infringe the reproduction right. Conclusively, the copier is the downloader who makes the copy. This provides a starting point when one examines the potential infringement of the exclusive reproduction right in the course of downloading.

Another important issue in the case of the exclusive right to make available to the public is the definition of 'public.' The meaning of 'public' does not include the close family and friends' circle of the user. However, the argument suggested by users of P2P networks that they do not communicate the work to the public, but they simply communicate it to their close circle of friends has been rejected because in the case of P2P file-sharing the exchange of file does not take place among individuals who are known or connected in another way to each other (*A&M Records, Inc. v. Napster, Inc.*, 2001). In the same spirit, the webpage where copyrighted works were posted was not considered a 'virtual private home', the

reproduction of the works there did not constitute reproduction for private use, and the fact that others could access the webpage did constitute communication to the public according to a French decision of 1996 (TGI Paris (réf.), 14 août 1996).

Therefore, arguably, the uploader could not take advantage of the private copy exception in the course of making a copy of the work since it cannot be said that he uses the work for his private use. However, a different answer may apply in the case when one uses one-click hosters and uploads the works and gives only to certain members of the public, i.e. his family and close friends, the URL to access this works (Westkamp 2007). Moreover, an issue is that the reproduction for private use provides an exception when the reproduction right, and not when the making available right, is infringed and a normative interpretation of the reproduction and the making available rights would mean that in the case of uploading there is an infringement of the making available right and that the exception that covers reproduction for personal use could not apply.

Apart from the above-mentioned issues, there are some specific issues regarding the making available right that arise in the context of the Bitorent technology due to the particularities of this technology. The Bitorent technology allows the works to be transmitted in small fragments. An argument, which is sometimes raised in favour of excluding the requirement of authorization to make works available, supposes that the partial or fragmented transmission of a work does not constitute an act of communication to the public. Even though this is an unsettled area of law, some writers argue that there is a communication to the public as soon as the individual makes the protected work available, on the open part of his hard disk, "regardless of the fact that only a few bytes of data are transmitted or that the file had been 'cut' and transmitted in 'packets' that travel different paths through the peer-to-peer system and when received are reordered and decoded by the computer of the downloader" (Bernault and Lebois, 2005).

Another particularity of the Bitorent technology closely linked to the above mentioned fragmented transmission of works is that every Bitorent user with a copy of the torrent files contributes a piece to the overall downloading. Where the making available of the work to the public and the reproduction of the work are happening simultaneously, the question arises whether the technically making available of the work to the public that takes place automatically when downloading the work (the downloader shares at the same time the work with others) infringes the making available right. The software that is used by the user does not give him the possibility to choose whether he will make available the work he is downloading to the public, but instead the making available takes place automatically while reproducing the work. In that case, the making available of the

work is 'passive' and it does not infringe the making available right since the user usually has not actual knowledge or the ability to control the making available of the work.

However, on the contrary it could be argued that there is infringement irrespectively of the actual knowledge of the user of his inability to control the actual dissemination of the work by way of analogy to the above mentioned argument that there is a communication to the public as soon as the individual makes the protected work available, on the open part of his hard disk. Even if one accepts a stretched interpretation of the communication to the public right, that a work may be communicated to the public in disjoined fragments, the Court in the *PirateBay* judgment stretched the meaning of the communication right even further to encompass situations where the technology is such that copyrightable works will actually never be downloaded from an individual user, but by numerous users simultaneously. In the view of certain writers, the Court has applied general criminal law principles and considered all participants in a 'swarm' to be accomplices of the same crime of communication to the public (Edstrom and Nillson, 2009).

### 1.3.2 Downloading

It has already been said that downloading infringes the reproduction right because it involves reproduction of the work without the rightholder's permission and that the person who copies is the downloader. In *BMG v Gonzales* and in *Napster* it was debated whether the users of P2P file-sharing networks can claim fair use of the work. In *BMG v Gonzales*, the defendant was downloading songs on her computer using the Kazaa P2P file-sharing network. The Court rejected the defendant's fair use defence that she was merely sampling songs with the intention to buy the ones she enjoyed. It was said that sampling musical works was not fair use since in that case it substituted purchased music and competes with licensed broadcasts and undermines the income available to authors. Instead, it was said that Gonzales could have listened to streaming music or sampled musical works from authorized and legitimate music services.

In *Napster*, it was held that the defendant, Napster, was liable for vicarious and contributory liability for infringement of the plaintiffs' copyrights. Both the District Court and the Court of Appeal held that Napster users were engaging in primary infringement of the plaintiffs' copyrights. In particular, it was said that sampling, where users made a temporary copy of the work to sample it before purchase was not fair use because it was in fact permanent and complete reproduction of the work. Space-shifting or works the users already owned to Napster was also not fair use because the work was made available to millions of other users as well and, therefore, the traditional shifting as fair use analysis found in

the *Betamax* decision or the *RIAA v Diamond Multimedia* decision did not apply in this case. The Court made a distinction between the legitimate practice of time-shifting and the illegitimate practice of library-building and downloading and retaining MP3 files instead of making ephemeral copies. It was also concluded that the Audio Home Recording Act 1992 does not cover downloading either.

In particular, in the Sony *Betamax* case, it was held that the making of individual copies of television shows for purposes of time-shifting does not constitute copyright infringement. In the *Diamond Multimedia*, *Diamond Multimedia* distributed the *Rio*, a device that allows a user to listen to MP3s through headphones. *RIAA* brought a suit to enjoin the manufacture and distribution of *Rio*. The District Court denied *RIAA*'s motion for a preliminary injunction finding that the Audio Home Recording Act 1992 exempted hard drives and computers and as such it did not apply to the *Rio*. The Appellate Court affirmed the District Court's denial of a motion for preliminary injunction because the *Rio* is not a digital audio recording device. The Court held that the *Rio* could only make copies from MP3s stored on computer's hard drives which were specifically exempted from the Audio Home Recording Act and that the *Rio*'s operation facilitates personal use in accordance with the Act's purposes.

In the EU, arguably, downloads will not constitute infringement if they fall within the scope of the private copy exception, as reformed after the implementation of the European Copyright Directive by the Member States. Regarding the proper scope of the concept of the private copy and 'private use,' if the user is only downloading and is not making files available to others, e.g. in the case of one-click hosters, then it could be argued that he could take advantage of the private copy exception. Moreover, the focus would not necessarily be on the private use of the copier since the concept of private use could also include a copy made in the family circle (Westkamp, 2007). In the same spirit, a German higher regional Court on Appeal recently dismissed a lower court verdict against *RapidShare*. *RapidShare* had been sued by rightsholders for distributing copies of movies and a lower court issued a preliminary injunction against *RapidShare*. The German superior regional court noted that *RapidShare* cannot control file uploads without possibly restricting local fair use laws (OLG Dusseldorf, Judgment of 22.03.2010). Regarding the private copying exception, the German higher regional court said that German copyright law allows users to make copies of music and movies for their own use, as well as to share them with a limited number of close acquaintances (§53 UrhG Reproduction for private and personal use) and that automated filters would make it impossible for users to save a legal back-up copy of a movie on *RapidShare*'s servers (OLG Dusseldorf, Judgment of 22.03.2010).

Two questions must be answered when examining the applicability of the private copying exception in the case of file-sharing networks. One question concerns the lawfulness of the source copy and another question concerns the satisfaction of the three-step test. Regarding the first issue, there is no definite answer. The lawfulness of the source is not an issue that must be considered when downloads are made from the Internet in Canada, France and Netherlands, while it is an issue in other countries, e.g. in Germany.

In particular, the Federal Court of Canada in a case between record companies and Canadian ISPs (*BMG Canada Inc. v. John Doe*, 2004) confirmed what had been proposed by the Canadian Copyright Board on copyright in its 2003 decision regarding the private copy exception (Copyright Board 2003). In particular, the Board had said that "(...) the regime is not about the source of the copy. Part VIII does not require that the original copy is a legal copy. It is thus not necessary to know if the source of the copy was owned by the copier, a borrowed CD, or a downloaded file from the Internet". The Federal Court said that "Under the Act, subsection 80(1), the downloading of a song for a person's private use does not constitute infringement". It was also said that "(25) Thus, downloading a song for personal use does not amount to infringement".

Regarding the infringing nature of uploading it was said that

(t)he mere fact of placing a copy on a shared directory in a computer where that copy can be accessed via a P2P service does not amount to distribution. Before it constitutes distribution, there must be a positive act by the owner of the shared directory, such as sending out the copies or advertising that they are available for copying.

However, on appeal, this conclusion was contested to the extent that it was said that conclusions regarding what would or what would not constitute infringement of copyright should not have been reached at the preliminary stages of the action, namely by the Federal Court (*BMG Canada Inc. v. John Doe* (F.C.A.), 2005).

In France, a computer sciences student was accused of copyright infringement for having reproduced on numerous CD-ROMs protected works downloaded from the Internet and for having made copies from CD-ROMs lent by friends. He then himself lent some of the CD-ROMs containing the reproduced works. Both the Rodez District Court and the Montpellier Court of Appeal held that the reproductions in question were covered by the private copy exception laid down in Art. L.122-5(2) of the French IP Code and, thus, acquitted the student (Wekstein, 2005). However, the Supreme Court accused the Appellate Court of not having taken into account the fact that the works reproduced had been made available

to the public by means of P2P software and of not having held on the lawful nature of the source as being a condition for the application of the private copy exception. It sent the case back to the Aix-en-Provence Court of Appeal which convicted the student of copyright infringement by holding that the private copy exception did not apply in this case since it generally does not apply “to the loan of CD-ROMs to friends” as these are third parties (CourCass, crim., 30 mai 2006). Unfortunately, the Aix-en-Provence Court of Appeal simply ignored the question of the lawfulness of the source (CA Aix-en-Provence, 5 septembre 2007; Thoumyre, 2007).

The reasons why the Aix-en-Provence Court of Appeal refused to hold on the lawfulness of the source requirement, although it was clearly invited to do so by the Supreme Court, are not clear. For example, it could be argued that the Court implied that the lawful origin of the work is irrelevant and that the French legislature could have decided to include it on the occasion of the copyright law reform following the model of Germany (Geiger, 2008). Irrespectively of the reasons behind this refusal, however, it has been argued that subjecting the application of all the copyright exceptions to the implied condition of the existence of a lawful source could be very problematic and “would call into question the equilibrium in copyright law,” since, for example, a student who reproduces a passage from an unauthorized text without would have qualified as infringer in such a case, even though the student might reasonably think the exception covered the reproduction (Geiger, 2008).

Generally, in 2005 the application of the private copy exception in the case of downloading works from P2P networks was confirmed several times by the French courts (Tribunal de Grande Instance de Bayonne, 15 novembre 2005; TGI Meaux, correctionnel, 21 avril 2005; TGI Paris, 8 décembre 2005). In one of these cases (TGI Paris, 8 décembre 2005), the French Supreme Court found the defendant not guilty both because his actions were exempted as reproduction for private use, and because there was also no infringement of the making available right. According to the Court, there is no element of bad faith in using P2P software and no evidence that the rightholders did not consent to the distribution of their works via P2P networks. It was accepted that the defendant when downloading the works simply placed a “copy” of the works in the shared folder to which the other users of the Internet have access without having previously checked the databases of rightholders whether he has the right to distribute their works and without knowingly infringing intellectual property rights. By accepting that the defendant simply placed a “copy” of the work in the shared folder, the Court implicitly accepts that the making available/distributing the work to the public is simply a technical consequence of the creation of a copy (which is, in turn, exempted under the reproduction for private use).

However, more recent French cases accept that the legality of the source could be a precondition for the application of the private copy exception. For example the Tribunal de Grande Instance de Rennes decided that the private copy exception cannot be applied when the source of the copy is illegal (TGI Rennes, 30 novembre 2006). Moreover, the Tribunal de Grande Instance de Montauban decided that user of the Kazaa software infringed the reproduction right and the making available right (TGI Montauban, 9 mars 2007).

In Netherlands, in a decision of 12 May 2004, the Court of Haarlem rejected the claim of Stichting Brein, a local associate against piracy, by refusing to hold liable the search engine Zoekmp3 for any infringement because it provided links to Internet sites from which music could be downloaded in the MP3 format without the authorization of the rightful owners (Brandner, 2004). According to the Court, the action of directing users to websites which offered, without authorization music files, was not illegal since, according to the websites, downloading of illegal files without sharing them is not contradictory to the copyright legislation (Brandner, 2004; Bernault and Lebois, 2005).

On the contrary, the lawfulness of the source explicitly determines the unlawful character of the download and precludes the application of the private copy exception in other countries. In Germany, for example, it was laid down on the occasion of the adoption of the law dated 10 September 2003 that the private copy exception did not apply when the original is an "obviously unlawful" source (Westkamp, 2007). The same approach is adopted by Portugal, Norway, Sweden and Finland (Westkamp, 2007).

With regard to the satisfaction of the three-step test in the course of downloading, the first criterion, 'certain special cases', arguably can be easily satisfied. In particular, the act of reproducing in the course of downloading could be considered a special case that could be exempted under the first step of the three-step test. The second step, however, namely the absence of conflict with the normal exploitation of the work, is more demanding and could wipe out the private copy exception in the context of file-sharing. There are two interpretations of the second step of the test that could apply here. First, the question is whether downloaded work affects the sales of works and the legal systems of downloading works, such as music and video, since studies on the subject are contradictory; in particular, some studies conclude that downloads affect sales, while some other studies reach the opposite conclusion (Oberholzer-Gee, Felix, and Koleman Strumpf, 2007; Liebowitz, 2006; Liebowitz, 2007; Andersen and Frenz, 2006; BPI Research & Information, 2009). Second, an interpretation of the three-step test suggests that the 'normal exploitation' would simply be ways by which it is

reasonable to believe that an author would exploit his work (Ricketson, 2003; Ricketson, 1998).

Regarding the first question on whether the sales of works are affected, one must be careful when interpreting the conclusions of the existing studies. Generally, it could be said that if rightholders lose money, it means that the users get for free something that they would have to pay for and, thus, the normal exploitation of the work is affected, and the other way round. Since the outcomes of the existing studies are contradictory, it would be better to follow the particular interpretation of the second step of the three-step test. Regarding this interpretation, it has been argued that there would never be a conflict with the normal exploitation of the work where there is no real possibility that the rightful owner could assert his right in prohibiting that exploitation or obtaining remuneration by free negotiation and contracting with users. Accordingly, downloads fulfill the second requirement of the three-step test because, in effect, authors and neighbouring right holders cannot practically control them, that is they cannot prohibit nor obtain remuneration using the individual management of rights, i.e. contracting with users.

Distributing works via P2P, however, would fail the third step since there would be “an unreasonable prejudice” to the legitimate interests of the rightholders. Therefore, in order to pass the third step of the test downloading should be the object of a compulsory license fee that compensates for a potential loss which prejudices the legitimate interests of the rightholders (Bernault and Lebois, 2005; Neil Weinstock Netanel, 2003; Fisher, 2004; Yu, 2005).

### **1.4 Conclusion**

Downloading may not infringe the exclusive reproduction right if it could be argued that the reproduction for private use applies. This could be argued, in principle, if there is no sharing of the work simultaneously, as is the case e.g. when one downloads from one-click hosters. The outcome, however, of a decision would further depend on the approach of a particular Member State regarding the issue of the lawfulness of the source. Regarding the satisfaction of the three-step test, arguably, downloads could pass the test if compensation methods are invented that are analogous to the remuneration, usually in the form of levies, that rightholders enjoy in the case of the reproduction for private use exception as applied in an analogue context. Uploading, however, would always infringe the making available right, unless it could be argued that it is done in the context of one-click hosters and the URL leading to the work is given to a restricted number of people. In sum, there is some scope for application of the reproduction for private use exception in the context of file-sharing networks that shows that maybe the exception should not be wiped out entirely in such a context but



instead file-sharing models that safeguard the exercise of the exception should be encouraged.

## References

Directive 2001/29 EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, Official Journal L167, 22/6/2001 P.0010-0019.

*A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9<sup>th</sup> Cir.2001).

Creative Commons (2009), 'Defining "Noncommercial" A Study of How the On-line Population Understands "Noncommercial Use" online at <[http://wiki.creativecommons.org/Defining\\_Noncommercial](http://wiki.creativecommons.org/Defining_Noncommercial)>/ accessed 05.02.2011.

Directive 2001/29 EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, Official Journal L167, 22/6/2001 P.0010-0019.

(5) See Rimmer M. (2007), 'Agent Smith and the matrix: copyright law and intermediary liability' in Rimmer M. (2007), *Digital Copyright and the Consumer Revolution: Hands off My iPod*, Edward Elgar, 190-224.

RIAA (2005), 'Music industry files new lawsuits in ongoing enforcement against online theft', Press Release, online at <<http://www.riaa.com/>> accessed 01.03.2011.

See IFPI (2006), Illegal music file-sharers targeted by fresh wave of legal action, online at <[http://www.ifpi.org/content/section\\_news/20060404.html](http://www.ifpi.org/content/section_news/20060404.html)>/ accessed 05.03.2011.

*Polydor Limited and Others v. Brown and Others* (2005) EWHC 3191 (Ch).

Institute for Information Law, University of Amsterdam, The Netherlands (2007), Study on the implementation and effect in Member States' laws of the Directive 2001/29/EC on the Harmonisation of certain aspects of copyright and related rights in the information society, Final Report, online at <[http://ec.europa.eu/internal\\_market/copyright/studies/studies\\_en.htm](http://ec.europa.eu/internal_market/copyright/studies/studies_en.htm)>/ accessed 10.12.2010.

Bernault, C. and Lebois, A (2005) A feasibility study regarding a system of compensation for the exchange of works via the Internet, Institute for Research on Private Law, University of Nantes, online at <<http://privatkopie.net/files/Feasibility-Study-p2p-acis-Nantes.pdf>>/ accessed 20.07.2010.

Hays T. (2006), The evolution and decentralization of secondary liability for infringements of copyright-protected works: Part I, E.I.P.R., 28(12), 617-624.

Staff Report Federal Trade Commission (2005), Peer-to-Peer file-sharing technology: consumer protection and competition issues, online at <<http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf>>/ accessed 20.07.2010.

Edstrom, Jerker and Nillson, Henrik (2009), The Pirate Bay verdict-predictable, and yet..., E.I.P.R., 31(9), 483-487.

Ficsor, M. (2006), Collective management of copyright and related rights in the digital, networked environment: voluntary, presumption-based, extended, mandatory, possible, inevitable?, in Gervais, D. (ed), *Collective Management of Copyright and Related Rights*, Kluwer Law International, 37-83.

Reinbothe, J. and Lewinski von S. (2002), The WIPO Treaties 1996, Butterworth's.

Ficsor, M. (2002), The law of copyright and the Internet, Oxford University Press.

*Football Dataco Ltd and others v Sportradar GmbH and another* (2010) EWHC 2911 (Ch); (2010) WLR (D) 293, Ch D: Floyd J: 17 Nov 2010.

Sydnor, Thomas D. (2009), The making-available rights under U.S. Law, The Progress & Freedom Foundation Progress on Point Paper, Volume 16, Issue 7, online at <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1367886](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1367886)>/ accessed 10.12.2010.

*Hotaling v. Church of Jesus Christ of Latter-Day Saints*, 118 F.3d 199 (4<sup>th</sup> Cir. 1997).

*Perfect 10 v. Amazon.com, Inc.*, 508 F.3d 1146 (9<sup>th</sup> Cir. 2007).

*Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539 (1985).

*London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153 (D. Mass. 2008).

*Elektra Entertainment Group v Barker* No. 05 CV 7340 (SDMY, filed 24 Feb. 2006).

*Atlantic Recording Corp. v. Howell*, 554 F.Supp. 2d 976 (D. Ariz. 2008).

*SONOFON A/S (formerly DMT2 A/S) v IFPI Danmark* Stockholm District Court, docket no. B 13301-06, judgment April 17, 2009 (the Pirate Bay case).

Manner, M., Siniketo, T. and Polland, U. (2009), The Pirate Bay ruling-when the fun and games end, Ent.L.R., 20(6), 197-205.

Wistam, H. and Andersson, T. (2009), The Pirate Bay trial, C.T.L.R., 15(6), 129-130.

TGI Paris (réf.), 14 août 1996, online at <<http://www.legalis.net>>/ accessed 20.12.2010.

Westkamp, G. (2007), Study on the implementation and effect in member States' Laws of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Final Report, Part II, The implementation of Directive 2001/29/EC in the Member States, Queen Mary Intellectual Property Research Institute, Centre for Commercial Law Studies, Queen Mary, University of London, online at [http://www.ivir.nl/publications/guibault/InfoSoc\\_Study\\_2007.pdf](http://www.ivir.nl/publications/guibault/InfoSoc_Study_2007.pdf) accessed 20.07.2010.

The District Court: *BMG et al. v. Cecilia Gonzalez* WL 106592 (N.D.III) (2005); The Court of Appeals for the Seventh Circuit: *BMG et al. v. Cecilia Gonzalez* 430 F.3d 888 (2005).

*Sony Corporation of America v Universal Studios, Inc* 464 US 417 (1984) (the Beta-max case).

*Recording Industry Ass'n of America v. Diamond Multimedia Sys., Inc.*, 180 F.3d 1072, 51 U.S.P.Q.2d (BNA) 1115 (9th Cir. 1999).

OLG Dusseldorf, Judgement of 22.03.2010, Az I-20 U 166/09, online at <http://www.telemedicus.info/urteile/1017-I-20-U-16609.html> accessed 20.01.2011.

*BMG Canada Inc. v. John Doe (F.C.)*, 2004 FC 488, (2004) 3 F.C.R. 241, March 31, 2004, T-292-04, online at <http://reports.fja.gc.ca/eng/2004/2004fc488/2004fc488.html> accessed 10.01.2010.

Copyright Board's, Private Copying 2003-2004 Decision, 12 December 2003, online at <http://www.cb-cda.gc.ca/decisions/> accessed 20.02.2011.

*BMG Canada Inc. v. John Doe (F.C.A.)*, 2005 FCA 193, (2005) 4 F.C.R. 81, online at <http://www.cippic.ca/documents/19May2005Ruling.pdf> accessed 20.02.2011.

Wekstein I. (2005), Téléchargement de films: Relaxe fuete de prevue d'un usage collectif des copies, CA Montpellier, 3<sup>ème</sup> ch. Correct.) 10 mars 2005, Légipresse, n.222, juin 2005, 120.

CourCass, crim., 30 mai 2006, RDL, juin 2006, 24-25.

CA Aix-en-Provence, 5 septembre 2007, RLDI 2007/31, n.1029.

Thoumyre L., Arrêt d' Aix-en-Provence du 5 septembre 2007: de la copie privée à la privation de copies? RLDI 2007/31, N.1025, 10.

Geiger Chr. (2008), Legal or illegal? That is the question! Private copying and downloading on the Internet, Case Comment IIC, 39(5), 597-603.

Tribunal de Grande Instance de Bayonne, 15 novembre 2005, Le Ministère Public et La SCPP c/ Monsieur D., online at <http://www.juriscorm.net> / accessed 20.07.2009.

TGI Meaux, correctionnel, 21 avril 2005, SPPF, SEV, SDRM, SCPP, SELL, SACEM, FNDF, FNCF c/ Stéphane, Rodolphe, Aleister, Aurélie, online at <http://www.juriscorm.net> / accessed 20.07.2009.

TGI Paris, 8 décembre 2005, Monsieur G. Anthony c/ SCPP, online at <http://www.juriscorm.net> / accessed 20.07.2009.

TGI Paris, (31<sup>ème</sup> ch.), 8 décembre 2005, online at <http://www.juricom.net> / accessed 03.03.2010.

TGI Rennes, 30 novembre 2006, SCPP et SPPF c/Madame A., online at <http://www.juriscorm.net> / accessed 10.03.2010.

TGI Montauban, 9 mars 2007, Le Ministère Public et La SCPP c/Madame M., online at <http://www.foruminternet.org> / accessed 20.03.2010.

Brandner S. (2004), MP3: télécharger n'est pas pirater, selon le tribunal d'Haarlem, online at <http://www.juriscorm.net/actu/visu.php?ID=511> / accessed 20.02.2011.

Oberholzer-Gee, F. and Strumpf, K. (2007), The effect of file sharing on record sales: an empirical analysis, *Journal of Political Economy* 115, No. 1, 1-42, online at <http://www.jstor.org/pss/10.1086/511995> / accessed 02.02.2011.

Liebowitz, Stan J. (2006), File-sharing: creative destruction or just plain destruction? Center for the Analysis of Property Rights Working Paper No. 04-03, online at <http://ssrn.com/abstract=646943> / accessed 20.02.2011.

Liebowitz, Stan J. (2007), How reliable is the oberholzer-Gee and Strumpf paper on file-sharing?, available at <http://ssrn.com/abstract=1014399> / accessed 20.02.2011.

Andersen, B. and Frenz, M. (2006), The impact of music downloads and P2P file-sharing on the purchase of music: a study for industry Canada, online at [http://www.ic.gc.ca/eic/site/ippd-dppi.nsf/eng/h\\_ip01456.html](http://www.ic.gc.ca/eic/site/ippd-dppi.nsf/eng/h_ip01456.html), accessed 20.03.2011.

BPI Research & Information (2009), The impact of illegal downloading on music purchasing, online at <http://www.ifpi.org/content/library/The-Impact-of-Illegal-Downloading.pdf> / accessed 20.01.2011.

Ricketson S. (2003), WIPO Study on limitations and exceptions of copyright and related rights in the digital environmnet, SCCR/9/7, online at <[http://www.wipo.int/meetings/fr/doc\\_details.jsp?doc\\_id=16805](http://www.wipo.int/meetings/fr/doc_details.jsp?doc_id=16805)>/ accessed 20.02.2011.

Ricketson S. (1998), International conventions and treaties, in Baulch L., Green M. & Wyburn M. (eds), *The Boundaries of Copyright, its Proper Limitations and Exceptions*, ALAI Journal of Studies, Cambridge, 3-26.

Netanel, N. W. (2003), Impose a noncommercial use levy to allow free peer-to-peer file sharing, *Harvard Journal of Law & Technology*, Volume 17, Number 1.

Fisher W. (2004), An alternative compensation system, in *Promises to Keep: Technology, Law and the Future of Entertainment*, Stanford University Press.

Yu, P. K. (2005), P2P and the future of private copying, *University of Colorado Law Review*, Vol. 76.

# YouTube, YouRisk, YouProtect - copyright issues

---

---

Maria Sinanidou

---

---

## Introduction

The popularity of user-generated content sites has grown exponentially in the recent years. As users are able to post photographs, articles, videos and music on Internet, user-generated content can consist of works partly or completely protected under copyright and be distributed online without the permission of the original rightholder. YouTube, the video-sharing website on which users can upload, share and view videos, is considered to be the dominant provider of online video in the United States and in Europe. While the wide range of topics covered by YouTube has turned video sharing into one of the most important parts of Internet culture, uncertainty surrounds the application of copyright rules to material uploaded on the Internet by individuals. Creators benefit from a bigger audience and market; consumers benefit from greater choice.

According to some data published by the market research company comScore, YouTube is the dominant provider of online video in the United States with a market share of around 43% and more than 14 billion videos viewed in May 2010<sup>1</sup>.

According to YouTube itself, 35 hours of new videos are uploaded to the site every minute and around 75% of the material comes from outside the US<sup>2</sup>. It is estimated that in 2007 YouTube consumed as much bandwidth as the entire Internet in 2000<sup>3</sup>.

- 
1. ComScore Releases May 2010 U.S. Online Video Rankings, available at <[http://www.comscore.com/Press\\_Events/Press\\_Releases/2010/6/comScore\\_Releases\\_May\\_2010\\_U.S.\\_Online\\_Video\\_Rankings](http://www.comscore.com/Press_Events/Press_Releases/2010/6/comScore_Releases_May_2010_U.S._Online_Video_Rankings)>. Retrieved May, 2011.
  2. 35 hours of video a minute uploaded to YouTube, available at <<http://www.google.com/hostednews/afp/article/ALeqM5hL4UMqXBKBTfj2PjHINPGpWZe82w?docId=CNG.7a039cc7305a51102e864beb3aa51545.181>>. Retrieved May, 2011, «Eric Schmidt, Princeton Colloquium on Public & Int'l Affairs», available in [http://www.youtube.com/watch?v=9nXmDxf7D\\_g#t=14m52s](http://www.youtube.com/watch?v=9nXmDxf7D_g#t=14m52s). Retrieved May, 2011.
  3. Carter, L. (April 7, 2008), Web could collapse as video demand soars. Daily Telegraph, available at <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/04/07/nweb107.xml>. Retrieved May, 2011. Charlie Bit My Finger is a viral video famous for formerly being the most viewed YouTube video of all time. It had over 245 million hits as of November 2010. The clip features two English

Compared to Napster and other file-sharing services, YouTube seems to provide better support to artists. Its present pre-publication service, for example, allows artists to decide whether they want to monetize their music or take advantage of the data of those who access their songs without authorization (in addition to blocking the use of their songs)<sup>4</sup>. From the standpoint of allowing artists to share in the profits, YouTube provides a significant improvement over file-sharing services.

On the other hand, one can still find a wide variety of criticism about YouTube, which range from a corporate control of culture to a lack of copyright protection and protection of privacy. Artists are concerned when incomplete versions of their work become available online without their prior consent. As Lars Ullrich, the drummer of the heavy-metal band Metallica, recalled: "One day I got a phone call telling me that this song we were working on ['I Disappear'] for this movie soundtrack [Mission Impossible 2] is being played on thirty radio stations in America, and I'm like, 'We haven't finished it yet. How did that happen?'" Although Ullrich has been much criticized for his legal actions against Napster, it is understandable that artists are disappointed when they loose control over their work<sup>5</sup>.

## I. YouTube

### 1. *What is YouTube?*

YouTube is a video-sharing website on which users can upload, share and view videos, created by three former PayPal employees in February 2005. Unregistered users may watch videos and registered users may upload an unlimited

---

brothers, with one-year-old Charlie biting the finger of his brother Harry, aged three. In Time's list of YouTube's 50 greatest viral videos of all time, "Charlie Bit My Finger" was ranked at number one.

4. As W. Patry described: A motion picture studio or other audiovisual content owner provides YouTube with a file of its work. YouTube then encodes the file; when a third party attempts to upload content that provides a match, YouTube contacts the studio and asks the studio what steps it wants to take. The studio can decide to block the upload, let the file be uploaded but tracked, or let the file be uploaded and run either contextual or its own advertisements against it, with the revenues generated being shared. An estimated 90% of content owners using video content identification have chosen to monetize their works, resulting in revenues that would not otherwise have been received. Even before the development of its video content identification, YouTube had in place a similar system for audio content contained in consumer-created videos, with an additional feature: Where an audio content owner objects to the use of the music, YouTube offers the user who created the video the ability to engage in an - audio swap. YouTube will, if requested, strip out the objected-to audio and replace it with a song that, either is in the public domain or licensed, thereby leaving the user-generated, no infringing video up for viewing, while respecting copyright owners' rights.

5. Yu P. K., Digital copyright and confuzzling rhetoric, see Footnote 115, p. 24.

number of videos. YouTube was bought in November 2006 by Google Inc. for \$1.65 billion and it now operates as a subsidiary of Google.

James Zern, a YouTube software engineer, revealed in an official blog post that just 30% of uploaded videos made up 99% of the views on the site. It means that 70% of the videos uploaded to the video sharing platform, bring little or no traffic and therefore make the company or its users little money in advertising revenue<sup>6</sup>.

The statistics raise questions over YouTube's model and suggest that the company is potentially spending too much transcoding and storing so many little-watched videos. YouTube makes most of its revenue from in - stream advertising on clips and programs from network and studio production partners, including Disney and film studio MGM. YouTube plans to deliver more premium video content to get existing users watching more content and subsequently drive traffic<sup>7</sup>.

According to the Italian newspaper *La Repubblica*, YouTube and other similar services based on user generated content (like Vimeo, Dailymotion, etc), will be considered under the Italian Law as broadcasters with the same obligations as the latter have. A key consequence is that these sites will be legally responsible for the content published by users. This obligation for YouTube to take the responsibility for the content published by its users facilitates the 500 million lawsuit of the Italian Prime Minister Berlusconi regarding publication of content protected under copyright of his TV networks. It is worth noting that the Spanish TV station of Berlusconi, *TeleCinco*, had defeated a similar case on the grounds that YouTube is not a producer of content<sup>8</sup>.

---

6. Almost all YouTube views come from just 30% of films, available at <<http://www.telegraph.co.uk/technology/news/8464418/Almost-all-YouTube-views-come-from-just-30-of-films.html>>. Retrieved April, 2011.

7. This scheme, which will reportedly cost the company \$100 million, has led some to question whether YouTube was leaving smaller users behind. However, it has been reported that the company did commit to investing in the next generation of talented online musicians and actors. YouTube NextUp in the UK will offer blossoming web stars support and promotion in their quest to become the stars of the future.

8. The Spanish court said it was the responsibility of the copyright owner to identify and tell Google when material that infringes intellectual property is on YouTube, noting that the site has tools allowing this to happen, see available at <<http://www.guardian.co.uk/technology/2010/sep/23/google-wins-youtube-case-spain>>. Retrieved May, 2011 and <[http://www.elpais.com/elpaismedia/ultimahora/media/201009/23/tecnologia/20100923elpeputec\\_1\\_Pes\\_PDF.pdf](http://www.elpais.com/elpaismedia/ultimahora/media/201009/23/tecnologia/20100923elpeputec_1_Pes_PDF.pdf)> for the whole text of the ruling, available in Spanish. Retrieved May, 2011.

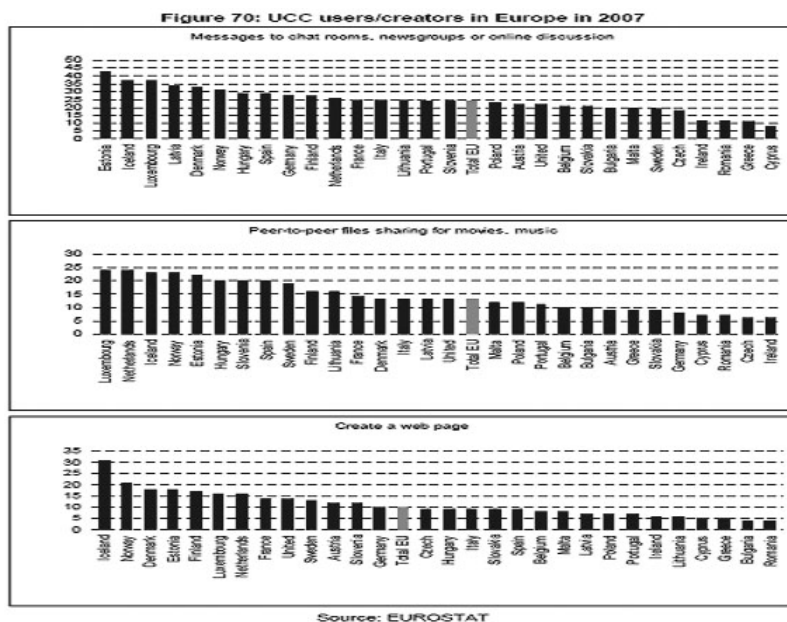


Apart from the list of most recently added videos, the website also offers listings based on different selection criteria such as 'featured', 'most discussed', and 'most viewed' lists, among others.

Methods are presented and experimental verifications on how the popularity of (user contributed) content can be predicted very soon after the submission has been made, by measuring the popularity at an early time<sup>9</sup>.

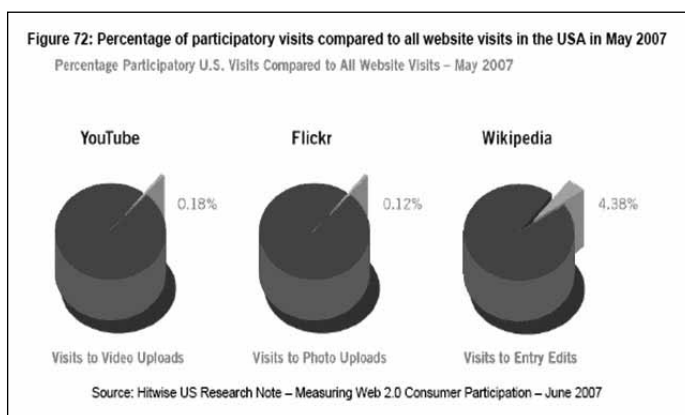
A survey of 13 EU countries published by the media communications agency Universal McCann in 2008 reported that there were wide variations in the upload activities. Although the proportion of the population in Britain and the Netherlands that has posted photographs online was 24% and 28% respectively, the proportion was only around 8% in Hungary, Poland and Greece<sup>10</sup>.

## Some statistics



9. Szabo G., Huberman B. A., Predicting the popularity of online content, available in <<http://ssrn.com/abstract=1295610>>.

10. Cronin D., User-created content shows uncertainty in EU copyright law, available at <<http://www.ip-watch.org/weblog/2008/11/07/user-created-content-shows-uncertainty-surrounding-eu-copyright-law/print/>>. Retrieved May, 2011.



## 1. Who are You? - The “players”

Facilitated by UGC (user generated content) platforms and technology in general, users can create an enormous amount of content, use and/or modify already existing content, etc. In the offline world it is quite easy to distinguish between the author, the editor, the publisher and the user. In the digital era and especially the UGC platforms this distinction gets a bit vague, as for example the user can, at the same time, become the creator and so, the copyright owner. The interest of an amateur or semi-professional user/creator in making profit from his work is not a premise for him to own copyright<sup>11</sup>.

### a. The creator/author

#### Originality and authorship

Not all UGC benefit from copyright protection in every EU country. Only original works deserve copyright protection. However, the concept of originality is not harmonized across the EU, which leads to the fact that the EU Member States apply different levels of originality ranging from the ‘skill and labour’ in the UK to the ‘print of the author’s personality that rises above average’ in Germany or to the ‘static singularity’ in Greece. Consequently, it may occur that some amateur photos, or videos maybe protected in a Member State and at the same time, not receive copyright protection in another Member State due to lack of originality<sup>12</sup>.

11. However, amateurs whose videos grow popular on YouTube seem to switch over to other platforms to generate revenues that enable them to earn a living by producing UGC, see IDATE – TNO – IViR 2008 User created content: supporting a participative information Society, Final Report, SMART 2007/2008, 166.

12. IDATE – TNO – IViR 2008 User created content: supporting a participative Information Society, Final Report, SMART 2007/2008, 158.

Platforms with user generated content like YouTube, Wikipedia, or Flickr involve various different authors who put their contribution up on the sites. This leads to the questions: Who is the owner of copyright in these works? What is the status in the sense of copyright of those works that constitute the content on those platforms?

The rules of ownership of rights on works created by multiple authors vary depending on whether such works are to be qualified as a «collective work» or as a «collaborative work». In the first case, the person who brings the contributions together to form a whole would be deemed the owner of the rights on the collective work, whereas, in the second case, the authors would be joint owners of the rights on the collaborative work. Whether the individual contributors to the collaborative work are able to exercise their rights on their own contribution without the consent of the co-authors depends on whether each contribution is separable from the whole or not.

All this, of course, holds true only in the absence of an agreement to the contrary.

These platforms would hardly qualify as a collaborative work, primarily because there generally would seem to be no common intention among the multiple authors to create a joint work. However, they would most probably not qualify as a collective work since the platform operators do not follow any creative editorial policy or exercise any control over the individual contributions that would be comparable to that of a conventional newspaper or encyclopaedia. As a result, each author is free to reproduce and communicate his work without the need to obtain the consent of the other authors<sup>13</sup>.

## **b. Special cases**

### *aa. in the course of employment*

Works are sometimes created in the course of employment. The rules regarding the ownership of rights on works created under employment vary significantly across EU Member States.

The law of countries like the UK, Ireland and the Netherlands expressly provide that the employer is the first owner of any copyright in a work made by an employee in the course of his employment, subject to any agreement to the contrary<sup>14</sup>.

---

13. IDATE – TNO – IViR 2008 User created content: supporting a participative Information Society, Final Report, SMART 2007/2008, 186.

14. Common Law System, see for the UK, for example, 45 CDPA, art. 11(2); the employer is treated as the first owner, but not deemed to be the author. Therefore the duration of copyright, for example, is measured with reference to the life of the employed creator.



*cc. the creator is under 18*

A large number of users of social networking and file-sharing sites are under 18. Contracts concluded with minors in the Netherlands can have legal validity on their own. In Germany, parental approval is required beforehand. In Greek copyright law, the legal capacity of the author and his desire for acquisition of copyright over his creation is not a prerequisite for copyright protection. Therefore, the copyright remains at the initial creator, even if he is a minor. The agreement is concluded on his name (as the rightholder) by the person(s) exercising his care.

**c. The user**

When the creator of the original work is the one who is uploading the visual part (video, photo) on YouTube there is, or at least should exist, no problem about infringement. The creativity of the author/creator and the originality of his work authorize him to use his creation as he likes, i.e. uploading it on YouTube. Thus, he should be careful about privacy. For example, if I take a video of nature and invest my creativity I may upload it on Internet and make it whatever I like. But, if I take a video of a concert, I might be allowed to film it (for my own use, for example if it is not prohibited) but not allowed to upload it. Or, if I take pictures of persons, even if one might call it art, it is not allowed to upload them on Internet without their consent. This video might be my creation so that I have the copyright on it, but there could arise some privacy issues.

When the work that the YouTube user is uploading is not his own, not only privacy issues, but also copyright issues arise (see under II, 1).

**II. YouRisk**

In October 2006, Google announced that it had acquired YouTube for \$1.65 billion, and the deal was finalized on November 2006<sup>20</sup>. At that time many wondered whether Google's decision was a risk, considering all pending lawsuits against YouTube for copyright and privacy law infringement.

YouTube users post their content directly onto YouTube servers, which gives them a similarly active role in facilitating access to infringing materials.

With its library of millions of video clips and simple embedding tools, it is easier than ever to display video on your site or blog including videos that might be infringing.

---

20. Greenmeier, L. and Gaudin S., "Amid the rush to Web 2.0, some words of warning Web 2.0 - InformationWeek" available at <[http://www.informationweek.com/news/management/showArticle.jhtml;jsessionId=EW RPGLVJ53OW2QSNLPC KHSCJUNN2JVN?articleID=199702353&\\_requestid=494050](http://www.informationweek.com/news/management/showArticle.jhtml;jsessionId=EW RPGLVJ53OW2QSNLPC KHSCJUNN2JVN?articleID=199702353&_requestid=494050)>. Retrieved May, 2011.

This raises the question about whether or not a site that posts an embedded clip could be held liable for it, especially if they were unaware of the infringement.

### **1. Legal Issues**

Since today Internet handles vast quantities of data, the statutory damages could be truly astronomical. Statistics show that more than 13 million hours of video were uploaded during 2010 and 48 hours of video are uploaded every minute, resulting in nearly 8 years of content uploaded every day. Over 3 billion videos are viewed a day and users upload the equivalent of 240.000 full-length films every week.<sup>21</sup>

Assuming 10 minutes per clip, that's 24 videos per minute, about 34.286 clips per day, or about 12.480.000 new videos per year. If only 1% of them infringe someone's copyright, YouTube could be liable for 124.800 works per year. Assuming \$10.000 in statutory damages for each of these, it would cost YouTube \$ 1.248.000.000 billion per year.

#### **a. Copyright**

In most cases, the creation and use of UGC is regulated by the general norms of copyright law. However, in some cases the terms of a license govern the exploitation and use of UGC.

As practise shows, the European legal framework in the field of copyright law leaves a lot of uncertainties for which the most important source comes from the lack of real harmonization in the area of copyright law within EU<sup>22</sup>.

Copyright is a form of protection provided for original works of authorship, including literary, dramatic, musical, graphic and audiovisual creations. Napster, and later Grokster, were both on the losing end of very large-scale copyright infringement lawsuits which resulted in both services being shut down. YouTube has also been accused of making available large quantities of works protected under copyright. With Napster and Grokster users could download a permanent copy of the media file. This violated the rightholders' right to control duplication of their work. YouTube streams its files, which does not create a permanent user

---

21. See <[http://www.youtube.com/static?hl=en&template=press\\_statistics](http://www.youtube.com/static?hl=en&template=press_statistics)>. Retrieved May, 2011.

22. See: European Commission's Internal Market Directorate-General (MARKT/2005/07/D) Study on the implementation and effect in member States' laws of directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, p. 18; P.B. Hugenholtz, M. van Eechoud, S. van Gompel et al., Recasting of Copyright and Related Rights for the Knowledge Economy, study prepared for the European Commission ETD/2005/IM/D1/95, Amsterdam, November 2006, online available at: <<http://www.ivir.nl>>.

copy. But file streaming can violate the copyright holder's right to distribute a work and the right to perform or display the work.

YouTube has a Copyright Centre with quite useful information on copyright issues<sup>23</sup>. As we read there, copyright infringement occurs when a copyrighted work is reproduced, distributed, performed, publicly displayed or made into a derivative work without the permission of the copyright owner. Posting copyright-infringing content can lead to the termination of ones YouTube account and possibly monetary damages if a copyright owner decides to take legal action. YouTube has also some guidelines to help users determine whether their video is eligible or whether it infringes someone else's copyright. YouTube states in its terms of use under section 5-G that *"YouTube is not responsible for the accuracy, usefulness, safety, or intellectual property rights of or relating to such User Submissions"*.

Uploading a digital file from a computer to the server computer is a reproduction in the sense of copyright law. Crucial is the storage on the server machine. When uploading a video file that contains the soundtrack in a copyrighted musical work, this musical work is being reproduced within the meaning of copyright. Reproduction may also exist when a work is being digitized in order to make it available to the public<sup>24</sup>.

YouTube has been criticized for failing to ensure that uploaded videos comply with copyright law. At the time of uploading a video, YouTube users are shown a screen with the message "Do not upload any TV shows, music videos, music concerts or advertisements without permission, unless they consist entirely of content that you created yourself". Despite this advice, there are still many unauthorized clips of copyrighted material on YouTube. YouTube does not view videos before they are posted online, and it is left to copyright holders to issue a takedown notice pursuant to the terms of the Digital Millennium Copyright Act (DMCA).

Organizations including Viacom<sup>25</sup>, Mediaset, and the English Premier League have filed lawsuits against YouTube, claiming that it has done too little to prevent the uploading of copyrighted material.

Within social networking and sharing communities, like YouTube or Flickr, it is not uncommon for makers of UGC to incorporate copyright protected third party

---

23. <[http://www.youtube.com/t/howto\\_copyright](http://www.youtube.com/t/howto_copyright)>.

24. The legitimate reproduction does not eliminate *ex tunc*. However digitization/reproduction may be illegal in case of circumvention of any TMP, see i.a. Vianello: Lizenzierung von Musik in nutzergenerierten Videos - Der steinige Weg zur Verwendung im Internet MMR 2009, 90.

25. 25 Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010).

content into their own works. Permission is required if the content is to be subsequently distributed, communicated or otherwise made available to the public, unless the third party content is in the public domain or the communication is covered by an exception or limitation. This is the case any time a user incorporates another author's song as background to his video, or uploads someone else's TV programme, video, film, text or photograph on his blog or on a platform like YouTube or Flickr.

The economic right of the copyright is subject to certain restrictions which are expressly provided by the national laws of the EU Member States. These restrictions in the copyright legislation are either in favor of the scientific progress or the information of the community and in a broader aspect in favor of the whole. These are cases where both a license from the author/rightholder and a fee payment are not necessary; such cases are expressly defined in law (for example, the right to make private copies, quotations, parody, public speeches, and news reporting, as well as the limitations to the benefit of educational institutions, libraries and disabled persons) and must be strictly construed.

## Case Law

### 1. Germany

The Regional Court of Hamburg<sup>26</sup> declined to issue a preliminary injunction against YouTube, which would have forced the site to remove 75 music videos in a conflict with 8 collecting societies (i.a. GEMA, ASCAP). However, the Court also said that the plaintiffs may actually have a right to ask YouTube to remove the unlicensed music videos and that the company indeed has some duty to take care of detecting illegal uploads. The only reason for the dismissal of the suit was that the collecting societies had known for a long time that the songs were available on YouTube without doing anything against it. So they only had the opportunity to ask for a ruling in regular proceedings.

In another case<sup>27</sup> brought by Frank Peterson, a German composer and producer for Sarah Brightman and other artists - the Regional Court of Hamburg issued a preliminary injunction against YouTube, ordering it to pay compensation after users uploaded several videos of performances by Sarah Brightman in violation of copyright laws. Google had pointed out that, since it asks users to confirm that they have the rights to upload the works they're uploading, it can't be held re-

---

26. <<http://justiz.hamburg.de/2479208/pressemeldung-2010-08-27.html>>. Retrieved May, 2011; see also *Journal of Intellectual Property Rights* Vol. 15, November 2010, pp. 486-493.

27. <<http://www.iuwis.de/blog/versch%C3%A4rfung-der-pr%C3%BCfpflichten-f%C3%BCr-plattform-und-forenbetreiber>>. Retrieved May, 2011.



sponsible for making sure that the content that the users upload is not infringing. However, the Court claimed that such a requirement doesn't absolve YouTube from liability.

## 2. Spain

In a Spanish case<sup>28</sup>, the Spanish broadcaster Telecinco had claimed that YouTube should be liable when users upload copyright-infringing material.

A federal court in Madrid, found that it is the responsibility of the copyright owners and not of YouTube, or Google, which owns it, to identify material that infringed copyright. The Court rejected Telecinco's claim calling the verdict "*a clear victory for the internet and the rules that govern it*".

## 3. USA

Internet and technology companies fear they would impair innovation and drive many of them out of business. Civil rights organizations argue the changes in the new technologies would damage an important new avenue of public communication<sup>29</sup>.

The DMCA established a carefully calibrated compromise between the rights of copyright owners and those of online companies. Among other things, section 512 DMCA established a safe harbor for online service providers mandating they would not be liable for storing or transmitting infringing material at their users' direction provided certain conditions were met. This safe harbor applies only if the online company does not know or should not reasonably have known about the infringement; and once the online company learns about the infringement, it must act 'expeditiously' to remove the infringing material.

Section 512 DMCA also created a notice-and-takedown regime. Copyright owners have a quick and easy way to notify online companies about infringing works. Online companies must respond to such takedown notices by expeditiously removing the allegedly infringing items from their Internet site or service. If an online company fails to do this, it loses its safe-harbor protection.

Users of online services receive some protection, too. When an online company removes allegedly infringing material that was posted by a user, that company is statutorily required to notify the user of what happened and why. The individual has a right to send a counter notification stating he or she has a 'good-faith belief' the material is not infringing. Once this counter notification is received, the

---

28. By the CNN Wire Staff, September 23, 2010.

29. <[http://www.abajournal.com/magazine/article/copyright\\_in\\_the\\_age\\_of\\_youtube/](http://www.abajournal.com/magazine/article/copyright_in_the_age_of_youtube/)>.

online company must put the disputed material back online within 14 business days, unless the company receives notice from the copyright owner that it has filed an infringement suit against the person who posted the material.

The *Io Group Inc. v. Veoh Networks Inc.* case raised the same issues of intermediary liability for copyright infringement and, ultimately, reaffirms the DMCA's safe-harbor protection for online companies.

Io Group makes and sells adult entertainment products including movies. Veoh Networks, like YouTube, allows users to upload and view videos online. Io alleged that clips from some of its movies were uploaded and viewed on Veoh, and that Veoh should be held liable for direct and secondary copyright infringement. Veoh argued that it was protected from liability by section 512(c) DMCA.

According to the U.S. District Court for the Northern District of California Veoh had no volitional control over its automatic copying and posting of uploaded material and the company could therefore not be held responsible for these actions. Veoh's users, and not Veoh itself, were the ones responsible for copying the clips and putting them onto Veoh's website. Thus, section 512(c) DMCA protected Veoh against copyright liability for those clips.

The Court rejected this argument, too. Judge Howard R. Lloyd held that although Veoh had the ability to control its own system, it did not have the ability to control the infringing activity. He concluded that the DMCA protects online companies like Veoh that work in good faith to limit copyright infringements committed by their users.

In another case in August 2008, a U.S. court ruled in *Lenz v. Universal Music Corp.*<sup>30</sup> that copyright holders cannot order the removal of an online file without first determining whether the posting reflected fair use of the material. The case involved Stephanie Lenz from Gallitzin, Pennsylvania, who had made a home video of her 13-month-old son dancing to Prince's song 'Let's Go Crazy' and posted the 29-second video on YouTube.

Viacom has alleged claims against YouTube for primary copyright infringement in the nature of public performance, public display, reproduction and distribution as well as secondary copyright infringement for contributory and vicarious infringement. Viacom has claimed damages in excess of \$1 billion<sup>31</sup>.

---

30. <[http://www.eff.org/files/filenode/lenz\\_v\\_universal/lenzorder082008.pdf](http://www.eff.org/files/filenode/lenz_v_universal/lenzorder082008.pdf)>. Retrieved May, 2011.

31. See Complaint at 48-97, *Viacom International, Inc., et al v. YouTube, Inc., et al.*, No. 1:07-cv-02103 (S.D.N.Y. Mar. 14, 2007).

One of Viacom's allegations is that YouTube is not policing its system as thoroughly as it can. According to Viacom's complaint, YouTube has filtering technology that can identify and possibly remove copyrighted material, but this technology is used to protect only works that are licensed to appear on YouTube - such as music videos of Sony BMG artists, clips from HBO shows and segments from MGM movies. Unlicensed works don't benefit from this technology, and their copyright owners thus face a flood of infringing posts.

ISPs and copyright owners have generally adapted to conducting business within the framework of the notice and takedown regime of the DMCA safe harbours<sup>32</sup>.

Viacom, demanding \$1 billion in damages, said that it had found more than 150,000 unauthorized clips of its material on YouTube that had been viewed 'an astounding 1.5 billion times'. YouTube responded by stating that it 'goes far beyond its legal obligations in assisting content owners to protect their works'. Since Viacom filed its lawsuit, YouTube has introduced a system called Video ID, which checks uploaded videos against a database of copyrighted content with the aim of reducing violations<sup>33</sup>. In June 2010, Viacom's lawsuit against Google was rejected in a summary judgment, with U.S. federal Judge Louis L. Stanton stating that Google was protected by provisions of the DMCA<sup>34</sup>. Viacom announced its intention to appeal the ruling<sup>35</sup>.

A U.S. District Court in New York ruled YouTube is covered by a 'safe harbor' clause in the DMCA that protects service providers from penalties for their users' copyright violations, so as long as they address those violations once they're made aware of them. According to Judge L. Stanton in the ruling of June 2010 'the provider must know of the particular case before he can control it'.

As presented above, Viacom, the owner of MTV Networks and Paramount Pictures, maintained that Google bought YouTube knowing full well that the site was guilty of copyright infringement but turned a blind eye to users' violations.

---

32. Strowel A., Peer to peer file sharing and secondary liability in copyright law, 2009, 240.

33. Read more under III. 4.

34. E-Commerce Law Reports, Vol. 8, Issue 6 (Mar. 2009), YouTube law fight 'threatens net'. BBC News, available at <http://news.bbc.co.uk/1/hi/technology/7420955.stm>>. Retrieved May, 2011.

35. Murph D., Viacom files appeal in YouTube Copyright case, continues to 'drag it out' in I:\ICIL\_20-21.5.11\Viacom files appeal in YouTube copyright case, continues to 'drag it out' -- Engadget.mht. Retrieved May, 2011 and Lefkow C., US judge tosses out Viacom copyright suit against YouTube, available at [http://www.google.com/hostednews/afp/article/ALeqM5h\\_AfErLSMMGD41718aR0CYib0aNQ](http://www.google.com/hostednews/afp/article/ALeqM5h_AfErLSMMGD41718aR0CYib0aNQ)>. Retrieved June, 2010.

According to the media company Google should review content before it is posted rather than waiting for copyright holders to request that Google remove illegal content.

U.S. District Judge J. Fogel of the Northern District of California held<sup>36</sup> that the DMCA requires copyright owners to consider fair use before sending a takedown notice. According to Fogel, if a copyright owner sends a takedown notice without first making a good-faith evaluation of whether the allegedly infringing work is covered by fair use, the owner could be liable for damages. The judge denied UMG's motion to dismiss the suit enabling Lenz to attempt to prove in an upcoming trial that UMG filed the takedown notice in bad faith.

The ruling is part of a larger legal struggle over who should bear the burdens of stopping online copyright infringement. Movie companies, record companies and many other copyright owners fear that - because committing copyright infringement online is so fast and easy, and because the huge number of online infringements is skyrocketing - it is impracticable for copyright owners to stop online infringements by suing all the individual wrongdoers.

Therefore, content owners are seeking alternatives such as trying to automate the process of removing allegedly infringing material or asking the courts to impose liability on YouTube and other online companies if these fail to vigorously police the material posted by their users.

While Viacom's long-standing copyright lawsuit against YouTube has gotten the most press attention, there's actually a second suit going as well - a class action brought by the Premier League and other major content owners saying that the giant video site's inattention to controlling copyright material violated the law. Now one big part of that class action suit, U.S. music publishers have bowed out of the case after striking a deal with YouTube.

The overall idea is to allow music publishers - the organizations that collect copyright payments for songwriters and composers—to identify videos on YouTube that use their compositions, and then get a split of YouTube's advertising revenue from the video. Record labels, which represent the artists that perform the songs, already have similar deals going. (Most music recordings have both a copyright on the sound recording and a separate copyright on the composition)<sup>37</sup>.

---

36. Seidenberg S., 'Copyright in the age of youtube, as user-generated sites flourish, copyright law struggles to keep up', available at [http://www.abajournal.com/magazine/article/copyright\\_in\\_the\\_age\\_of\\_youtube/print/](http://www.abajournal.com/magazine/article/copyright_in_the_age_of_youtube/print/). Retrieved May, 2011.

37. Mullin J., 'Music publishers settle with youTube, as other defendants fight on', available at <http://paidcontent.org/article/419-limewire-settles-with-music-publishers-but-keeps-fighting-record-labels/>. Retrieved May, 2011; see also Tutt P., 'Music publishers settle

Viacom finds YouTube more acceptable now that it has incorporated software filters. Viacom's case, like the class action, is being argued on appeal.

#### **4. France**

Interesting is also a case from France, that does not involve YouTube, nevertheless is about hosting sites. In a decision from 17.02.2011<sup>38</sup> the French Supreme Court recognized the hosting status of Web 2.0 services Dailymotion and Fuzz.fr. The Court also confirmed, in relation to the Amen website case, that the judges had to verify that the content withdrawal requests observed the requirements of LCEN (loi pour la confiance dans l'économie numérique - French implementation of the EU E-commerce Directive) before condemning a hosting site that had not withdrawn promptly the notified content.

According to LCEN, the request to withdraw content must cover a series of elements including the notification date, the identification data of the notifying person (either natural or legal), the identification data of the addressee, the description of the litigious facts and precise location, the reasons for the withdrawal including legal basis and justification, a copy of the correspondence addressed to the author or editor of the litigious actions asking for their interruption, withdrawal or modification, or the justification of the fact that the author or editor could not be contacted.

The decisions of the Court of Cassation establish clearly the boundary between a content hosting site and a web service editor. In the Dailymotion case, it comes to confirm the decision of the French Court of Appeal of May 2009 which overturned a 2007 court decision that considered the hosting site liable for the content posted online on its platform. Moreover, the site had responded immediately after having been notified that it was hosting illegal content.

The Court of Cassation also overturned the decision against Fuzz.fr in the case introduced by actor Olivier Martinez. In 2008, a French court decided that the owner of the website had an editorial responsibility, even if the website was a digg-like service (where the users can vote which news comes on first) and forced him to pay 1000 euro in damages for infringing the actor's privacy and an additional 1500 euro in legal fees. The Court of Cassation considered fuzz.fr a hosting site in terms of LCEN and therefore not liable for the content posted on it.

---

YouTube suit', available in: <[http://blogs.ft.com/fttechhub/2011/08/music-publishers-settle-youtube-suit/?utm\\_source=twitterfeed&utm\\_medium=twitter#axzz1Vfx4xsKB](http://blogs.ft.com/fttechhub/2011/08/music-publishers-settle-youtube-suit/?utm_source=twitterfeed&utm_medium=twitter#axzz1Vfx4xsKB)>. Retrieved August, 2011.

38. See <http://www.edri.org/edriagram/number9.4/french-supreme-court-cases-fuzz-dailymotion>> with further references.

An important clarification in relation both to Dailymotion and the Amen hosting site is the necessity to correctly formulate the requests for content withdrawal by taking all actions stipulated by law.

A hosting site cannot be required to withdraw content before proving that the author of the content has been first contacted and required to withdraw the respective content. This could be the end of mass withdrawals of files without any previous procedure.

However, the Legal Commission of the Senate seems to want to change the rules and on 15.02.2011 proposed the creation of a new status between host and editor that will have filtering and surveillance obligations.

## **5. Belgium**

Google found itself in hot water when its keyword advertising service was accused of promoting copyright piracy by 'selling' keywords such as 'bootleg movie' and 'pirated'. And in February 2007 Google's Belgian Website was ordered to stop showing excerpts of Belgian newspaper articles on its Google News sites due to copyright concerns<sup>39</sup>.

### **b. Privacy**

YouTube as well as other similar services have been raising, beyond copyright, also privacy concerns. What if I post a video that contains images of other people? Am I liable to them for invasion of their privacy? More importantly, is YouTube liable for invasion of privacy? What if the situation involved criminal activity? Should YouTube be compelled to release my name as the poster of the video and, if so, under what circumstances? Commentators are beginning to cast a careful eye on these questions with the answers slow in coming.

The lack of transparency in the use of personal data and content is a growing concern. Users are concerned about how their passively or actively created data or content is used - or will be used in the future. National governments lack the means to reinforce their general consumer protection policies or to negotiate efficient alternatives for UGC platforms. This lack of instruments to regain control over one's privacy - including the right to be left alone - becomes clear in the few cases in which very personal content grows into a media sensation.

---

39. <<http://www.edri.org/edriagram/number5.3/google-belgium> with further references>.

On May 23<sup>rd</sup> 2011, there was an event in the International Press Centre in Brussels hosted by ECIPE<sup>40</sup>. As it has been said there<sup>41</sup>, politics and governments were dividing the Internet. With regard to EU, preaching of freedom across the world would not have the desired effect if EU did not implement this freedom in its own legal system.

It has been also noted that Google's business depends on the free flow of information. As regards current challenges, indicative is the recent Italian YouTube case, in which three Google employees were convicted of privacy violations because students at a school in Turin uploaded a video to YouTube that showed the bullying of an autistic child. In this particular case, *convicting Google employees was the same as making a postman for carrying the contents of the post*<sup>42</sup>.

### III. YouProtect

YouTube has developed The YouTube Copyright Workshop, a self-paced guide aimed to familiarize creators and users with key copyright terms and ideas such as copyright infringement, copyright ownership, penalties, authorized use, fair use, YouTube's copyright tools.

In the ongoing copyright debates, areas of common ground are seemingly few and far between. One belief that unites many stakeholders across the spectrum is that more efforts are needed to educate Internet users about copyright. Internet has spawned legions of amateur content creators, but not all of the content that's being created is original. Indeed, a great deal of online copyright infringement owes to widespread ignorance of copyright law and its penalties.

Google unveiled on April 16<sup>th</sup> 2011 'Copyright School' for YouTube users: users whose accounts have been suspended for allegedly uploading infringing content will be required to watch this video and then correctly answer questions about it before their account will be reinstated. It will be interesting to see how Google's effort influences the behavior of YouTube users and the incidence of repeat infringement.

The entertainment industry should not ignore the fact that these new platforms have provided an exciting environment, where users mix their content with pre-

---

40. ECIPE Study in <<http://www.ecipe.org/digital-authoritarianism-human-rights-geopolitics-and-commerce/PDF>>. Retrieved May, 2011.

41. See <<http://www.edri.org/edriagram/number9.11/foe-european-internet>> with further references.

42. Internet FoE: how should Europe battle online censorship? available at <<http://www.edri.org/edriagram/number9.11/foe-european-internet>>. Retrieved May, 2011.

existing works - copyrighted or otherwise. While some uses of these preexisting contents - such as the unauthorized verbatim reposting of music videos or comedy clips - are undoubtedly infringing, others - such as the posting of originally created home videos with no underlying copyrighted content - are clearly legal. Even more complicated, in between these two categories are those uses whose copyright status remains unclear - thanks to the many limitations and exceptions in the copyright system, such as fair use<sup>43</sup> *de minimis* use exception<sup>44</sup> and the limited scope of derivative work right.

Moreover, social networking platforms have opened the door for the public to actively participate in cultural production. The potential for such participation is indeed a main reason why commentators have pushed for greater accommodation of cultural participation in existing copyright law.

Creative reuse and modification of pre-existing materials, therefore, are highly valuable to society. They ensure that everyone has a fair chance to participate in the production of culture, and in the development of the ideas and meanings that constitute them and the communities and subcommunities to which they belong<sup>45</sup>.

As netizens learn to reuse and modify preexisting works, there inevitably will be *good* remixes and *bad* remixes<sup>46</sup>.

### **1. How can you protect your work?**

Copyright law provides tools for the protection of the rightholder and his work. In EU Member States, but also on an international level, there are several tools such as civil, criminal and even administrative sanctions for those who infringe ones copyright.

The notion of registration does not exist in copyright law, as for example in the industrial property law. The rights arising from copyright law begin to exist once the work is created and assumes a specific form. Therefore, no formal procedure is necessary on the part of the author - e.g. the submission of the work to a public institution, its registration to a special registry, the payment of a specific fee, etc. - in order for him to be able to exercise his author's rights. The inclusion of the

---

43. See 17 U.S.C. § 107 (2006).

44. See *Newton v. Diamond*, 388 F.3d 1189, 1192–96 (9th Cir. 2004) (discussing the *de minimis* use exception).

45. Balkin J. M., Digital speech and democratic culture: a theory of freedom of expression for the Information Society, Yale Law School, Faculty Scholarship Series. Paper 240, available at: <[http://digitalcommons.law.yale.edu/fss\\_papers/240](http://digitalcommons.law.yale.edu/fss_papers/240)>.

46. Yu P.K., Digital copyright and confuzzling rhetoric, see p. 9.



© sign in copyright material does not play any part in the origination of the right and it neither adds nor removes anything as far as copyright issues are concerned.

However, for the purpose of securing the author and having a proof of authorship, in effect there are two practices that are usually followed<sup>47</sup>. The first one is the submission of the intellectual creation before a notary. The second practice followed is to send a registered letter having both as sender and addressee the author himself or another addressee, retain the receipt and maintain the letter, which will include the work, unopened until and if a difference arises regarding the specific work, in which case the letter will be opened before court by a judge, who will certify its content.

Both practices act as proof and serve as disputable evidence (which means that they can be counter-evidenced) for the fact that, at the particular point in time, the work had already been created by the author, and they can be used if a problem arises and a third party claims ownership of the author's work. Both practices are simple, common procedures that can be used to certify the document's date. It is in the judge's discretion to evaluate the probative value of these actions<sup>48</sup>.

Further to the law, the rightholder can use technological measures protection, i.e. technological tools in order to restrict the use or access to his work.

## ***2. How do I make sure my video does not infringe your copyright?***<sup>49</sup>

Some platforms – and most notably YouTube – have signed agreements with a long list of content providers including CBS, BBC, Universal Music Group, Sony Music Group and others. In Europe, there are also examples of license agreements between UGC's and collecting societies; for example between YouTube and GEMA, and the Dailymotion and the Société Civile des Producteurs de Phonogrammes en France<sup>50</sup>.

---

47. In most EU Member States both of these practices are common. This is something that does not derive from the law itself but is commonly used and acknowledged.

48. In Greece, if none of the above actions has been taken by the author, he can refer to any other piece of evidence that might exist in accordance with the general rules of the Civil Procedure Code, in order to prove his authorship.

49. See for more: Bailey J., copyright risks in embedding YouTube clips in the blog Herald available at <<http://www.blogherald.com/2007/07/09/the-copyright-risk-of-embedding-youtube-clips/>>.

50. Cabrera Blazquez F.J., 'User-generated content services and copyright', IRISPlus, 2008-5, pp. 2-8, p. 6; 'YouTube wheels and deals to avoid copyright suits', The Associated Press, October 10, 2006, available at: <The Associated Press, October 10, 2006, <http://www.law.com/jsp/article.jsp?id=1160397318970>>.

In cases where no global agreement has been reached between the platform operator and content providers, users should clear the rights on third party content that they upload. Obtaining permission imposes transaction costs, such as the costs of establishing the copyright status of the work, the costs of identifying, locating and contacting the right owner, and the costs of negotiating with the right owner to obtain a license to reproduce or otherwise use the work. In some cases, these costs can be so high that prospective users either renounce in actually reutilising the work or prefer running the risk of facing a claim for infringement. Especially for amateur and semi-professional creators, who form the biggest share of individuals active on UGC platforms, the difficulty of tracing the right owners on third party content so as to obtain permission may appear as an insurmountable obstacle<sup>51</sup>.

Some platforms license selected user created content in order to include it in their music (radio) and video streams, whereas others will license professional content. The Dailymotion has launched the Official Content programme inviting official content to be shared via its site. In addition, the Dailymotion has concluded licensing agreements with e.g. Universal Music and Warner Music. It, moreover, has closed deals with several professional news organizations including Le Figaro, Le Monde, Libération, France Info, Rue89 and France 24 to post content on the site<sup>52</sup>.

Some of the larger UGC platforms show clear tendencies to move into the direction of multi-media content distribution platforms. YouTube has struck numerous partnership deals with content providers such as CBS, BBC, Universal Music Group, Sony Music Group, Warner Music Group, NBA, The Sundance Channel.

There are some simple precautions one can take to make certain he doesn't infringe ones copyright. If the user creates something completely original, then his video doesn't infringe someone else's copyright. YouTube offers a library of authorized music to liven up ones video<sup>53</sup>. There are many websites that have cop-

---

51. User-created- content: supporting a participative Information Society, Final Report, SMART 2007/2008, IDATE, TNO, IVIR 2008, 197.

52. (for more information see Part III, section 2.2.3 of the Study: User-created- content: Supporting a participative Information Society, Final Report, SMART 2007/2008, IDATE, TNO, IVIR 2008).

53. One potential new model that made headlines in recent years was the release of the album 'In Rainbows' by Radiohead. The band released the album online and allowed users to pay what they wanted – including nothing at all – for the music during the first several weeks of its release. Another band, Nine Inch Nails, later released two albums under a Creative Commons license, see more in Mara K., Panellists: copyright law's 'byzantine maze' stalling new business models in IP watch, 9.11.2010.

right-free images and texts such as Wikipedia. Taking material from those sites helps you avoiding copyright infringement.

It is also important to follow the terms of use.

If the user plans to link to another site and offers a summary of that site's information, he might ask in advance whether or not he can use their material, especially if he intends on an ongoing use<sup>54</sup>,

Though linking is not a guaranteed way to avoid being sued for copyright infringement, it is definitely preferable to embedding. If you are unsure about a video clip, consider linking to it rather than embedding it directly. Many major rightholders have official YouTube channels that allow embedding.

### **3. YouTube and rights administration**

One of the biggest issues in copyright is the administration of the rights. It is being said that in almost every country collecting societies often resist telling YouTube what they own and that there is no publicly available database that provides this information.

YouTube has recently sealed a deal with RightsFlow, a music publishing rights management company to help address the complexities around music rights management. RightsFlow is a licensing and royalty service provider for artists, record labels, distributors, and online music companies. The company specializes in rapid song identification in particular, as well as in "*obtaining bulk physical, DPD and ring-tone licenses including streaming, tethered and limited download rights*"<sup>55</sup>.

According to an agreement between YouTube and RightsFlow, YouTube is allowed to enlist RightsFlow's help in processing and managing music rights.

In case of piracy, Google's expected attitude actually gives priority to 'legitimate' content distribution services, initially in terms of music or video.

Google will respond within 24 hours to reliable requests to remove references to pirated content, initially in the search results of Google and Blogger (to improve the process for submitting requests from copyright holders, claims relating to breach of DMCA, i.e. to use methods to circumvent the protection of copyright works by copying). At the same time, Google will improve the tools for those who believe that Google has wrongly responded to such request, and remove the

54. See latest case on live streaming on <<http://www.iposgoode.ca/2011/08/does-live-streaming-infringe-copyright/>>. See also latest decisions in Greece from TriPlimKilk 965/2010 in DIMEE 2/2011, 194, MPrAth 4042/2010 in DIMEE 2/2011, 195 with further references.

55. See more at <<http://rightsflow.com/who-we-are/about-rightsflow/>>.

references to the services or content. All requests to remove references to content and services will be public and searchable.

Conditions considered to be closely related to piracy will not appear on autocomplete<sup>56</sup>. Google seems to admit a weakness of the search engine because *“it is difficult to identify with certainty that the search terms are being used to violate copyright”*. Thus Google states that it will do everything it can not to propose those terms by the auto-complete search terms.

No AdSense ads will appear on websites that are considered as piracy sites, so that it is not considered that advertising on Google eventually supports piracy. Basically Google will respond to requests from copyright rightholders who indicate a site that is making their work available to the public without their consent and will remove the ads from these sites.

Google will make efforts to promote in the search results ‘legitimate’ content and services, even if it is about previews (a few seconds of music, movie trailers, legal services of selling music, etc). To this end, Google proposes to copyright rightholders to give a unique identity to their creations, the so called Content ID. The decision is based on the assertion that most users want access to legal content and interested in their Shuttle offer, even if it is preview.

#### **4. YouTube’s role in protection**

At the end of 2007 YouTube introduced a technology called Video ID, which allowed copyright owners to compare the digital fingerprints of their videos with material on YouTube, then flag infringing material for removal. Instead of demanding their material to be taken down, media companies opted massively to the alternative offered by the technology. Companies can ‘claim’ the videos and start showing ads alongside them, creating a new revenue stream for both YouTube and the content owners. According to David King, a product manager at YouTube, 90% of the copyright claims made using the identification tool remain

---

56. Autocomplete is a feature provided by many web browsers, e-mail programs, search engine interfaces, source code editors, database query tools, word processors, and command line interpreters. Autocomplete involves the program predicting a word or phrase that the user wants to type in without the user actually typing it in completely. This feature is effective when it is easy to predict the word being typed based on those already typed, such as when there are a limited number of possible or commonly used words (as is the case with e-mail programs, web browsers, or command line interpreters), or when editing text written in a highly-structured, easy-to-predict language (as in source code editors). Autocomplete speeds up human-computer interactions in environments to which it is well suited. Autocomplete features are often enabled by default, and disabling or defeating them can sometimes be difficult for users to accomplish.

on the site and are converted to advertising inventory. The other 10% are either removed from the site or tracked by the content owner. YouTube says the claiming process had more than doubled the number of videos that its 300 Video ID partners can monetize, but the total number is still small, since ads would appear on less than 3% of video pages<sup>57</sup>.

With respect to audiovisual content, rights clearance and the existence of a one-stop-shop solution is less problematic. However, an easy and affordable access for online platforms such as Youtube.com could form their services into legal offers. This would call for multi-territorial or at least Europe-wide license models and sustainable fees.

But Google representative Luc Delany refuted allegations that YouTube is flouting the law. Whenever it is notified that video clips on the service are subject to copyright, Google takes one of three courses of action, he said. The first option would be to delete the material. The second would be to monitor its use; this can prove beneficial, he contended, to film-makers who could decide if it would be worthwhile releasing a movie in a particular country based on whether people there are viewing promotional trailers for it on Internet. And the third would be to offer financial recompense to the rightholder by giving it some of the money gained from online advertising.

YouTube started rentals in early 2010 with films from Sundance that barely registered. By April, it had more than 500 partners and 'hundreds' of films for rent from \$ 0.99 - \$ 3.99 and a year later it's up to 'thousands'. It is being argued that to compete with iTunes, YouTube needs the same inventory or at least the same window and it also needs to sell more people on the notion that YouTube is the best place to watch movies - especially paid movies<sup>58</sup>.

Executives at Fox and Paramount have said they want Google to do a better job of clearing pirate sites out of their search results, and apparently they want to put the brakes on YouTube renting out their content until they see better progress<sup>59</sup>.

---

57. Read more at < [http://news.cnet.com/8301-1023\\_3-20051539-93.html#ixzz1JP6vdgIW](http://news.cnet.com/8301-1023_3-20051539-93.html#ixzz1JP6vdgIW)> and in: 11 Cf. New York Times, August 16, 2008, 'Some media companies choose to profit from pirated YouTube clips'.

58. Kramer S.D., 'YouTube on the verge of a big movie upgrade?', available at: <<http://paidcontent.org/article/419-youtube-on-the-verge-of-a-big-movie-upgrade/>>. Retrieved May, Retrieved May, 2011.

59. The service may start as early as this week or next, and is expected to be announced soon by YouTube. Major studios including Sony Pictures Entertainment, Warner Brothers and Universal have licensed their movies for the new service, as have numerous independent studios, including Lionsgate and the library-rich Kino Lorber, according to movie executives with

Every week hundreds of thousands of people embed YouTube videos of their favorite artists on websites, but they're not paying for these broadcasts. Music royalty collection agencies are known for going to extremes to claim money on behalf of artists and music composers.

In 2008 there was a heated debate in The Netherlands where the local royalty collection agency announced plans to charge website owners for embedding music videos from YouTube. After massive protests from the public the plan was cancelled, and the royalty agency closed a private deal with YouTube directly.

More recently the Slovak royalty collectors SOZA started sending fines and invoices to bloggers. Everything started in May 2011 when a local blogger posted that SOZA tried to fine him for embedding YouTube videos on his blog. They further asked for 16.60 Euro/month for a licence to publish YouTube videos on his blog. This has sparked a revolt among Internet users. A storm of negative comments followed, and eventually it also got the attention of mainstream media. After this SOZA acknowledged they had made a mistake and acted wrongfully and unlawfully. They returned all the money collected from bloggers, who are again free to embed YouTube videos<sup>60</sup>.

On December 2<sup>nd</sup> 2010 extremely important news emerged when Google took a clear position against piracy. Google and YouTube will hereinafter promote only legitimate services of music and film distribution. Torrent sites will be deleted from their indexes.

---

knowledge of the deals in place. YouTube has been laboring to bring all the major Hollywood studios on board before announcing it, according to one executive involved in the deal. But so far Paramount, Fox and Disney have declined to join. The service is the biggest studio VOD deal since all the major studios signed on to Apple's iTunes rental service in January 2008. Fox, Disney, Warner Bros., Paramount, Universal, Sony, MGM, Lionsgate and New Line were all on board for that initiative. The site's 130 million monthly users will be able to pay to watch movies as they come out into the DVD market; it is the first serious foray by the Google-owned company into mainstream movies and charging money for video. The executive said that Hollywood studios were excited by having a tech giant like Google involved in a new streaming service, with the hope that the parent company would develop new technologies to encourage sell-through purchases of movies that could be securely stored in a digital locker. See also Mullin J., 'Two studios hold out on YouTube movie rental deal - piracy is the issue', available at <[http://paidcontent.org/article/419-three-studios-hold-out-on-youtube-movie-rental-deal-piracy-is-the-issue/?goback=%2Egde\\_63465\\_news\\_495091666](http://paidcontent.org/article/419-three-studios-hold-out-on-youtube-movie-rental-deal-piracy-is-the-issue/?goback=%2Egde_63465_news_495091666)>. Retrieved May, 2011.

60. 'YouTube embed royalty results in public outrage', available at <<http://torrentfreak.com/youtube-embed-royalty-110621/>>. Retrieved June, 2011.

## Conclusion

The arrival of YouTube, Facebook, MySpace and other social networking platforms has shown the immense creative potential of netizens. Much of this potential, however, does not depend on the incentives generated by the existing copyright system. While policymakers and commentators have yet to reach a consensus on the appropriate standards for treating user-generated content, there is no doubt that the creation of this new type of content has inspired innovative thinking about the development, dissemination, and exploitation of creative works.

The European Broadcasting Union (EBU)<sup>61</sup> stated in a White Paper entitled, 'Modern Copyright For Digital Media: Legal Analysis and EBU Proposals' that, although it fully supports the protection of copyright and related rights, the current EU legal framework on rights clearance "needs to be modernized", so that it is more efficient and the offering to European media will be improved<sup>62</sup>.

Among the proposals, EBU aims to "facilitate EU-wide online licensing through the concept of audiovisual media communication to the public," as well as "clearance of retransmission rights for any platform," according to the principle of technological neutrality, where a policy should not favor a particular technology.

EBU also advises avoidance of 'separate rights for the same activity'. That refers to rights being granted by contract or by law to communicate content to the public, which it said should also cover incidental reproductions necessary in the exercise of the license, and the general adoption of the 'extended collective licensing' model' to clear rights for audio and audiovisual media services. Proposals also include the simplification of music licensing for audiovisual media services providers, the use of collective licenses for unlocking broadcasters' archives, and the supervision of collecting societies<sup>63</sup>.

---

61. The EBU has members from 56 countries in and around Europe and promotes public service media in Europe and around the world. The EBU report was authored by S. Edwards, P. Kamina and K.-N. Peifer.

62. European Broadcasters Call For Easier Copyright Clearance For Online Content By Catherine Saez in Intellectual Property Watch, 17.03.2010.

63. Extended collective licensing has been in use in Denmark since the 1960s with satisfactory results. Under this model, DR has an agreement with an umbrella organization of collecting societies who represent a substantial number of rights owners. This agreement is also applied for authors who are not represented by a collecting society; they are given the same remuneration, he said. Under this agreement, DR will be able to give access to all archives and broadcasts, containing fiction, drama and news to Danish citizens, after digitalization. It's a win-win situation," he said, with a new stream of revenue for authors, and access to "all this content" for the public. The authors can opt out if they prefer their production not to

The protection and enforcement of copyright is important. Also creation in all its form needs incentives. Modern means of creation should not be hindered by any rules as long as this creation respects the fundamental rights of privacy, freedom of expression and copyright. Thus, it is important to differentiate work from simple information; work requires creation and originality.

YouTube is part of the copyright ecosystem. Merely because some users abuse copyright, it does not mean that YouTube is illegal. The law is clear in this sense. Technology will always be a step ahead from the law. The aim is to find solutions within the existing system of international treaties and the established *acquis communautaire* of copyright law. It seems that we need a copyright regulatory environment in Europe with a uniform concept, thus ensuring easier access to quality content.

---

be broadcasted, the spokesperson said. The agreement is only permitted for non-commercial use of the archives, he said.



# From online diaries to online 'unmonitored' media?

---

---

Evgenia Smyrnaki

---

---

## 1. Introduction

Internet serves as a precious medium of information and exchange of ideas. However, misuse leads to violation of public interest and rights of third parties, facilitating illegal activities<sup>1</sup>. Copyright infringements, child pornography, racist content, violation of privacy rights are only some of the activities public authorities are trying to effectively combat and accordingly regulate.

Blogging is a computerized form of writing opinions, ideas, news online. They started as online diaries used for uploading one's thoughts. Now they have evolved into medium of information, which many recognize as today's mainstream media tending to substitute the traditional (offline and online) ones. As a matter of fact, blogs have even been characterized as a new form of journalism<sup>2</sup>, since no high capitals and expensive equipment is entailed for their operation. A computer, on Internet access, and a free blogging program are enough for aspiring amateur journalists who want to make the difference<sup>3</sup>. However, the determination of their legal status has been in the centre of discussions and many contradictory thoughts have been expressed.

A characteristic example of the controversies relating to blogging is given by the recent Greek case of a TV channel which filed an action against a blog and a journalist who they claimed to be the blog's operator. The language used in an online survey of the blog asking readers to vote on who of the journalists of the channel favored more the government was considered as offensive by the plaintiffs. Blogosphere was bombed by hundreds of messages, expressing their opposition towards the suit. Freedom of speech, anonymity, and the role of bloggers in society conflicted with the right to one's reputation and honor. The online and offline

- 
1. Kastanas Hel, Internet and the protection of privacy and freedom of expression: in query of smart provisions, in *New Technology and Constitutional Rights (Law and Society in the 21<sup>st</sup> century)*, 2004, p. 31 (in Greek).
  2. Ribstein E. L., From bricks to pajamas: The law and economics of amateur journalism, 48 *WM & Mary L. Review* 185, 187 (2006).
  3. Ciolly A., Bloggers as public figures, 16 *B.U. Pub. Int. L.J.* 255, 2006-2007.

turmoil resulted in a team of hackers attacking the channel's portal, demanding the withdrawal of the action. The hackers tried to clarify that they defended freedom of speech without specifying whether they agree with that blog or not<sup>4</sup>.

Blogs operating under the veil of anonymity are considered as a threat to freedom of speech and democracy, which should be based on outspokenness, equality before law and equal speech. They are said to be anything but 'citizen' journalism since they are managed by 'specific journalists', while at the same time a new genre of journalists who think of codes of conduct as something bad, is bred<sup>5</sup>. Others recognize the value of Internet as a tool in the hands of young people, accepting at the same time that words irrespective of the environment they appear in –either offline or online– still can be insulting. It is suggested that the extinction of such phenomenon should not be the product of state force or intrusion, but rather a product of education. The fact that members of a society do not realize that one's freedom stops where the other's begins, depicts a failure of the system and society, something worse than the offensive/ defamatory content itself<sup>6</sup>. On the other hand, there are those in favor of cyber-anarchy, defending a free of state control and unprincipled online world.

Absent clear and harmonized law provisions on anonymity and state of bloggers, courts are left with the difficult task to attempt to reconcile all implicated and conflicted interests.

## 2. Freedom of speech and expression

*"First they came for the communists,  
And I didn't speak out because I was not a communist.  
Then they came for the trade unionists,  
And I didn't speak out because I wasn't a trade unionist.  
Then they came for the Jews,  
And I didn't speak out because I was not a Jew.  
Then they came for me  
And there was no one left to speak out for me"*

Pastor Martin Niemoelle

Freedom of expression, speech and press is established in many legal documents. Article 10 of the Rome Convention for the protection of human rights and fun-

---

4. <<http://www.eglimatikotita.gr/2011/03/mega-fimotro.html>> (in Greek).

5. Pagkalos Th., Information and press in the era of blogs, 23/04/2011, Kathimerini Newspaper, <[http://news.kathimerini.gr/4dcgi/\\_w\\_articles\\_columns\\_3\\_23/04/2011\\_439985](http://news.kathimerini.gr/4dcgi/_w_articles_columns_3_23/04/2011_439985)> (in Greek).

6. Kanakis Ant., Blogs: Freedom or not?, 10/04/2011, [www.aixmi.gr](http://www.aixmi.gr) (in Greek).

damental freedoms, states that everyone is free to hold opinions and to impart information and ideas without the interference by public authority and regardless of frontiers. In USA, First Amendment mandates that Congress shall make no law abridging the freedom of speech or of the press. If a State enacts content based regulation, it is considered as unconstitutional<sup>7</sup>. In Greece, article 14 of the Constitution addresses that everyone has the right to express and propagate his thoughts orally, in writing and through press in compliance with the laws of the State. Censorship and other preventive measures are prohibited. Likewise, article 5A of the revised Constitution states that everyone is entitled to information and is entitled to participate in the Information Society. The right introduced by article 5A underlines the obligation of the State to facilitate free access of people to the services and all potentials offered by the Information Society. This right is of a double nature. It is both a personal and social right, guarantying the participation of people in a social environment under formation<sup>8</sup>.

However, the protection of free speech is not absolute. All above provisions include conditions under which the freedom is restricted. Rome Convention highlights that the freedoms are combined with several duties and responsibilities. They may be subject to such formalities, conditions, restrictions and penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity and public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of reputation or rights of others, for preventing the disclosure of information received in confidence or for maintaining the authority and impartiality of the judiciary. In USA the Supreme Court has categorized several categories of speech which do not deserve protection (e.g. child pornography) or deserve limited protection (advertising speech). However, First Amendment offers stronger protection to free speech. For instance, public figures enjoy limited protection by law in connection to defamation claims. Even press is not held liable, unless the plaintiff-public figure proves that the journalists acted *with actual malice*. As the Supreme Court noted in *New York Times v. Sullivan*: “[D]ebate on public issues should be uninhibited, robust, and wide-open, and it may well include *vehement, caustic, and sometimes unpleasantly sharp attacks* on government and public officials”.

In Greece, restrictions can be imposed by law, as long as they are absolutely necessary and justified on national security grounds, for combating crime or for protecting rights and interests of third parties. Free speech is not protected in case the conditions of defamation (Art. 363– Greek Penal Code) are met (false state-

---

7. Fotiadou Alk., Balancing the freedom of speech, Sakkoulas, 2006, p. 31 (in Greek).

8. Kofinis St., Participation in Information Society as a new constitutional right, DIMEE 4, 2007, p. 515 (in Greek).

ment, knowledge of the falsehood). In case someone uses offensive and insulting language, he is immune from liability if he had a justified interest to do so (Art. 367- Greek Penal Code). The kind of the interest is not defined by law. For instance, it may be of a public, private, moral, economic or professional nature. However, it is another issue whether the court will accept the interest<sup>9</sup> and where it will draw the crucial line, over which freedom of expression is not justified and the protection of other lawful rights prevails.

Expression which is protected under the above provisions and conditions includes writing, oral expression of thoughts, opinions to the other members of the society. Writing even in emails, in Braille language, on every material like cars, walls etc amounts to written expression<sup>10</sup>. Written expression enjoys further constitutional protection if it is considered as press<sup>11</sup>. Written depiction of thoughts in words, in graffiti, by signs on walls is indeed expression of opinion but cannot be considered as press<sup>12</sup>. Blogging involves writing one's thoughts and ideas online and constitutes written expression. The question posed is whether it can be classified as press as well, since the provisions applied in case of press defamation/ libel disputes are special and differ from the common ones.

### 3. Blog = Press?

In several cases brought before the Greek Courts, plaintiffs asked for the stricter Press Law provisions to be applied to bloggers. Law 1178/1981 provides that the owner of a newspaper must compensate the libel victim, even if the author of the disputed article is unknown. Lower limits of compensation are determined for the owners (10mill. dr. for daily issued papers in Athens and Thessaloniki, and 2mill. for other papers). Courts in the following cases: Court of First Instance (Polymeles Protodikeio) in Thessaloniki 25528/2010<sup>13</sup>, in Piraeus 4980/2009<sup>14</sup>, Court of First Instance in Rodopi 44/2008<sup>15</sup> have ruled that bloggers are not operators of press and must not be subject to the strictest provisions of the Press

---

9. Chatzikostas, *Insults against honor due to justified interest*, Sakkoulas, 2005, p. 57 (in Greek).

10. Dagtolgou, *Human and social rights*, Sakkoulas, 2005, p. 494 (in Greek).

11. Greek Constitution article 14.

12. Dagtolgou, *Human and social rights*, p. 570 (in Greek).

13. Polymeles Protodikeio (Court of First Instance) in Thessaloniki, 25552/2010, DIMEE 2010/4, p. 515 (in Greek).

14. Polymeles Protodikeio (Court of First Instance) in Piraeus 4980/2009, DIMEE 2010, p. 101 (in Greek).

15. Monomeles Protodikeio (Court of First Instance) in Rodopi, Armenopoulos, 2009/406. (in Greek).

Law. The technical and organizational characteristics of blogs were considered by Courts.

Blogs are closely interconnected and from an online community, the blogosphere. They are seen as a means of expressing oneself freely and in an interactive way, which differentiates them from other online or offline papers. Technically, the Internet user can write comments under the main post of a blog and engage in an online conversation with each other and with the blogger himself. Posts appear chronologically with the most recent to be first. In addition, in newspapers there is editorial control of the articles, whereas in blogs everyone can reply. It shall be noted however, that in some blogs the operator controls which comments are to be posted. Blogs aim at the exchange of thoughts and not primarily in disseminating news. Most of them include news from all sectors of everyday life (life-style, politics, gossip, tv, sports etc) like other online media. Yet blogs don't give the sense of press to its readers. Most of them consider it as an unofficial and more subjective view of every day issues. Blogs have become really popular among readers which rely most on blogs than other official news sites.

The high compensation is another reason why press law must not be applied to blogs. Big undertakings usually own the press and the capitals invested are high. The owner of the press has the financial means to defend himself or just pay the compensation. Press law would have a devastating effect on the economic existence of bloggers and a chilling effect on free speech. High compensations would intimidate bloggers to freely express ideas. It is disproportionate to allow a press law to apply to e.g. a simple student who operates a blog. However the fact that application of press law in blogs is excluded does not mean that bloggers are immune from any liability. Traditional law provisions on protection of personality, privacy, defamation are applied (e.g. articles 59, 920, 914 of the Greek Civil Code, art. 361-369 Penal Code).

However, the analogous application of press laws, may in some jurisdictions depend on the degree of leniency the provisions may offer to bloggers. In the French case *Maire d' Orleans Serge G. vs Antoine B.- blogueur*, Serge G. candidate for the elections in Orleans filed an action against a blogger Antoine B., who acted under the pseudonym of Fansolo and who turned out to be a candidate of the opposite party for the elections as well. The defendant created a blog named "les amis de Serge G." using photos of the plaintiff without having his consent, making many spelling mistakes, presenting his programme and commenting on acts from his past in a rather satiristic and humoristic way,

eventhough it was supposed to support him<sup>16</sup>. The plaintiff's claims were upheld both by the Tribunal de Grande Instance d'Orléans<sup>17</sup> and the Court of Appeal.

The interesting point in this decision is the fact that the blogger invoked the law provisions applicable to press. He argued that his acts fell within the ambit of the Law of the Freedom of the Press of 29 July 1881 (Press Law) and not under article 1832 of the Civil Code and that the plaintiff's claim was not that of tort but of abuse of freedom of expression. Press law deals with defamation cases in an effort to consider both the freedom of the press and the rights of the individuals. Based on articles 53 and 55 of press law, Fansolo asked for dismissal of the plaintiff's claim, on the grounds that he had not abided by the strict provisions as to the service of the action and the deadlines. According to the Court, the blog did not contain defamatory content which is a prerequisite for the application of the press law to be applied but rather aimed to held him up to ridicule. It is worth mentioning that despite the fact that the Court applied the regular tort law based on the characterization of the blogger's acts ('deffamation', 'injure' or 'denigrement') and not on the nature of the medium used, the Court of First Instance highlighted that it is possible that a blog may benefit from the same protections offered to press if specific conditions are met<sup>18</sup>. Further, the Court of Appeal indicated that the blogger did not have the right to benefit from the protections of press law without adhering to certain duties such as transparency since he was acting *anonymously* in order to discredit a rival politician<sup>19</sup>.

---

16. Cour d'appel D'Orléans Chambre civile Arrêt du 22 mars 2010 Antoine B. / Serge G. available at <[http://www.legalis.net/spip.php?page=jurisprudence-decision&id\\_article=2919](http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2919)> (accessed 29/04/2011): 'les articles publiés sur ce blog se livraient à une présentation critique, sous un angle satirique qui se voulait humoristique, de l'action passée, du programme et de la personne de Serge G. qu'il était censé soutenir'.

17. Tribunal de grande instance d'Orléans Ordonnance de référé 08 octobre 2008 Serge G. / Antoine B. available at <[http://www.legalis.net/?page=jurisprudence-decision&id\\_article=2912](http://www.legalis.net/?page=jurisprudence-decision&id_article=2912)> (accessed 29/04/2011).

18. 'Attendu qu'il peut être admis qu'un blog peut bénéficier dans certaines conditions des mêmes protections que la presse mais qu'il n'y a pas lieu d'examiner ce point en l'espèce sauf à faire observer que la loi sur la presse détermine des conditions très spécifique sur l'identification de l'organe de presse'. Tribunal de grande instance d'Orléans Ordonnance de référé 08 Octobre 2008 Serge G. / Antoine B.

19. 'Attendu qu'à titre superfétatoire, la Cour ajoutera qu'Antoine B. est assez malvenu de vouloir bénéficier des droits protecteurs qu'accorde la loi de 1881 sans supporter, aussi, les devoirs que celle-ci impose, en matière de *transparence et de loyauté*, aux organes de presse alors qu'il a agi de façon *anonyme* et sous une présentation trompeuse pour discréditer un adversaire politique;' Cour d'appel D'Orléans Chambre civile Arrêt du 22 Mars 2010 Antoine B. / Serge G.

#### 4. Anonymity

As has been highlighted by Recommendation 99 (5) for the protection on privacy on the Internet, anonymity is the most appropriate way to safeguard privacy online<sup>20</sup>. However, legally, complete anonymity is not feasible. The use of pseudonyms is suggested so that only the ISPs know the true identity of online users. In addition, ISPs are advised to inform users of programmes allowing them to browse anonymously online (R 99(5), III For ISPs). Nowadays, rapid rise in online illegal activity has directed regulations towards online transparency at the expense of privacy and the right to anonymity.

In England, anonymity of bloggers is said to be 'killed'<sup>21</sup> by a 2009 ruling of the High Court of Justice (*The author of a blog v. Times Newspaper Limited* (2009) EWHC 1358 (QB)<sup>22</sup>). The author of the blog 'Night Jack' (a serving police officer) sought an interim injunction to prevent the Times to reveal his identity, which Times had discovered through a process of deduction and detective work based on information available online. Times had already revealed his identity to the police service and the blogger wished to prevent any release of his personal information to the public, readers of Times. The blogger claimed that the Times had an enforceable duty of confidence not to reveal his identity and that he enjoyed a reasonable expectation of privacy, since there was 'no counterveiling public interest justification' for the publication of his identity. His blog dealt with police issues and stories, and depicted the blogger's thoughts and views on political and social issues. So, a revelation of his identity, as he argued, would probably make him liable for breach of police regulation relating to confidentiality which would subsequently result in his freedom of expression being restrained. The Court relied on the test adopted in *Napier v. Pressdam Ltd*<sup>23</sup> (2009) where it was stated that: "For a duty of confidentiality to be owned (other than under a contract or statute), the information in question must be of a nature and obtained in circumstances such that any reasonable person in the place of the recipient ought to recognize that it should be treated as confidential. ...Freedom to report the truth is a precious thing both for the liberty of

20. Council of Europe, 1999, available at <<https://wcd.coe.int/wcd/com.intranet.InstraServer-vlet?command=com.intranet.CmdBlobGet&IntranetI%20mage=276580&SecMod e=1&DocId=396826&Usage=2>>.

21. Gibb Frances, Ruling on NightJack author Richard Horton kills blogger anonymity, The Times, June 17, 2009, <[http://technology.timesonline.co.uk/tol/news/tech\\_and\\_web/the\\_web/article6509677.ece](http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article6509677.ece) (accessed 29/04/2011)>.

22. Available at <[www.westlaw.co.uk](http://www.westlaw.co.uk)>.

23. *Napier and another v. Pressdam Ltd*, Court of Appeal 19 May 2009, [2009] EWCA Civ 443 [2010] 1 W.L.R. 934 (available at [westlaw.co.uk](http://www.westlaw.co.uk) – accessed 29/04/2011).

the individual (the libertarian principle) and for the sake of the wider society (the democratic principle), and it should be unduly eroded if the law of confidentiality were to prevent a person from reporting facts which a reasonable person in his position would not perceive to be confidential."

However, the Court concluded that the public's right to learn the particular source of the comments and Times' right to freedom of expression to unmask the identity of the blogger prevailed over the claimed right of blogger's privacy, since blogging is more of a public than a private matter. But the above is not the only case indicating that there is little expectation of privacy and anonymity where posting on blogs and anonymously. In 2007, BBC revealed the true identity of the owner of the political blog 'Guido Fawkes', following a 2005 attempt by the Guardian newspaper<sup>24</sup>.

In Germany, Media Providers are obliged to offer identification information on their websites (Impressum page) as long as their sites do not operate exclusively for personal or familial purposes (Art. 55, RStV)<sup>25</sup>. In addition, article 5 of the Telemediengesetz mandates that business-like ("Geschäftsmaessig") Telemedia service providers should provide name, address, e-mail, commercial register, VAT number<sup>26</sup>. The above regulation - in force since 1.3.2007- adds up to legal uncertainty<sup>27</sup>. The issue which arose is whether bloggers must include an Impressum in their blog, since even the appearance of *banners*, or the use of *Google Adsense*, would render blogs the *business-like* trait.

A concrete answer cannot be provided. Rather the design and specific characteristics of blogs must be considered accordingly on a case by case basis. This was the

24. Tumbridge James, Twitter: who's really there?, *Journal of Intellectual Property Law and Practice*, 2010, vol. 5, no. 2, p. 117 (available at <http://jiplp.oxfordjournals.org>), accessed 14/02/2011).

25. Article 55 – Informationspflichten und Informationsrechte, Staatsvertrag ueber Rundfunk und Telemedien (RStV), available at <http://www.juraforum.de/gesetze/rstvni/55-rstv-informationspflichten-und-informationsrechte>: "Anbieter von Telemedien, die nicht ausschließlich persönlichen oder familiären Zwecken dienen, haben folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten: 1. Name und Anschrift sowie 2. Bei juristischen Personen auch Namen und Anschrift des Vertretungsberechtigten."

26. Article 5 – Telemediengesetz, "§5 Allgemeine Informationspflichten: (1) Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten: ...", available at <http://www.telemediengesetz.net/>.

27. Dr Stephan Ott, Die Impressumspflicht nach § 5 TMG / § 55 RStV, available at <http://www.linksandlaw.info/Impressumspflicht-Notwendige-Angaben.html>.



outcome of a decision of Koeln's Landgericht<sup>28</sup>. The two plaintiffs filed a suit on copyright claims against the provider of a software platform which provided Internet users the technical and storage infrastructure to create blogs. A user of the platform, who had created his own blog, published some photos of the plaintiffs. One of the arguments posed by the plaintiffs was the absence of an Impressum by the blog. The Court concluded that the disputed blog was not subject to such a disclosure obligation under par. 55 RStV. The purpose of the blog as 'personal' proved to be the crucial factor. The Landgericht highlighted that the term *personal* ('Persoenlich') refers to the scope of communication and not to the nature of the communicated subject itself. It depicts the need for personal communication of political opinions, personal anger or disappointment<sup>29</sup>.

In USA, it is interesting that anonymous bloggers are notified when an order is sought to reveal their identity. The ISP must (e.g. by using the email of the blog's registration) provide the blogger with notice of the proceedings. Then the blogger can appear anonymously at court through counsel and submit opposition papers. Anonymous bloggers appearing at court are called John Does. In *Cohen v. Google*, the anonymous blogger argued that the provocative photographs and words ('skank', 'ho') posted on the blog about the model Cohen, were 'non-actionable opinion and/or hyperbole' and that they were not verifiable statements of facts. She further added that the blogs 'have evolved as the modern way soapbox for personal opinions'- an argument the Court rejected by quoting a Virginia Court statement that although Internet is an inexpensive means of communication, "the dangers of its misuse cannot be ignored. The protection of the right to communicate anonymously must be balanced against the need to assure that those persons who choose to abuse the opportunities presented by this medium can be made to answer for such transgressions"<sup>30</sup>. The Court ordered Google to provide all information that would assist in ascertaining the identity of that person or persons.

---

28. LG Koeln – Urteil vom 28. Dezember 2010, 28 O 402/10, available at <<http://openjur.de/u/149188.html>>.

29. "‘Persoenlich’ bezieht sich nach dem Wortlaut auf die Zwecke der Kommunikation, nicht etwa auf das behandelte Thema. Persoenlich ist der Zweck der Kommunikation aber auch dann, wenn der sich Aeussernde dem persoenlichen Beduerfnis nach Kommunikation politischer Meinungen, persoenlichen Aergers oder Entaeuschung nachkommt. ... Der streitgegenstaendliche Blog entspricht hiemach dem Schutzzweck des Gesetzes und der ratio der Ausnahme von der Informationspflicht einer Internetforum und faellt daher nicht unter die Informationspflicht des 55 Abs. 1 RStV. Denn der anonyme C1 gibt seine persoenliche Meinung zu bestimmten Themen Bekannt, wie dies auch bei Meinungauesserung in Foren der Fall ist.", available at <<http://openjur.de/u/149188.html>>.

30. *Cohen v. Google Inc.*, Supreme Court of the State of New York, 17-08-2009, available at <<http://www.citmedialaw.org>>.

In Greece, confusion prevails regarding the requirements to be satisfied for disclosure of identities. On one hand law 2225/1994 mandates that confidentiality is refused only where specific crimes listed therein have been committed such as defamation/ libel, use of offensive, insulting language or threats. However, three opinions issued by the prosecutors of the Supreme Court (Areios Pagos) – 9/2011, 12/ 2009, 9/ 2009-, indicate that the right to anonymity, privacy and non-disclosure of information does not extend to crimes of defamation, offensive and insulting language and threats. The scope of the law on confidentiality is the protection of private written communication. Defamatory, offensive, threatening content is of criminal nature and does not constitute private communication so as to deserve protection. Service providers have to make a choice, either disobey a prosecutors order and not disclose information, or disclose the information, violate law 2225/1994 and face the danger of fines from independent authorities, such as DPA, or Hellenic Authority for Communication Security and Privacy (www.adae.gr)<sup>31</sup>. It is urgent that Greek legislators dilute the uncertainties by taking a firm, uniform and clear stance on the matter.

As a matter of fact, Greek Minister of Justice has created a law drafting committee assigned the task of drafting provisions on bloggers' identification and reviewing the crimes for which confidentiality is refused<sup>32</sup>. Still, fears are expressed that from now on bloggers will have to provide their names unconditionally.

The name, identity of an individual are classified as *personal* data protected against any unauthorized processing. Anonymity may reflect a right or '*self-centered need*' of an individual but, at the same time, identification of an individual satisfies another need, that of social nature, since the individual co-exists with others<sup>33</sup> – either online or offline. It is suggested that the right to anonymity **cannot be interpreted as a right to social irresponsibility**<sup>34</sup>. A minimum of personal data for tracing a person must be available<sup>35</sup>. However, anonymity must not be refused on mere **preventive grounds**. Such a provision would be dispro-

---

31. It is worth noting that State Prosecutor's Opinion 9/2011 was issued after law 3917/2011 came into force. Provisions of law 2225/1994 were repeated in law 3917 for the retention of electronic communication data. However, the State Prosecutor in his opinion 9/2011 confirmed that the previous two opinions are still valid.

32. Kathimerini, "Creation of law drafting committee on blogs", 05-08-2011, available at <[http://portal.kathimerini.gr/4dcgi/\\_w\\_articles\\_kathbreak\\_1\\_05/08/2011\\_401345](http://portal.kathimerini.gr/4dcgi/_w_articles_kathbreak_1_05/08/2011_401345)>. The Law drafting committee is expected to have completed its work by 30/09/2011. (in Greek).

33. Stathopoulos M., Use of personal data and the fight among freedoms of the data holders and freedoms of the data subjects, Nomiko Vima, January 2000, vol. 1, p. 9 (in Greek).

34. Stathopoulos M., *ibid*.

35. Stathopoulos M., *ibid*.

portionate and impair free expression, comments and criticism. Bloggers should still have the right to write anonymously and only if specific illegal activity has already taken place, then the authorities would be authorized to proceed to disclosure of their identity for crime **investigation purposes**. In any case, refusal of anonymity is not the ultimate solution to problems of criminal activity online. As a matter of fact, there are and will always exist easy, inexpensive ways to circumvent any measures intended to fight anonymity. The internet user with a simple use of a proxy site, software or server is capable of participating in forums, chats, social networks under the veil of anonymity without being traced.

## 5. Microblogging: Twitter

Twitter is a communications medium, which has been characterized as a microblog, though each message cannot exceed 140 characters. Anonymity on Twitter cannot be guaranteed either. The initial terms and conditions on privacy provided for the disclosure of information even to private parties, where Twitter at its sole discretion, believed to be “*necessary or appropriate to respond to claims, legal process (including subpoenas), to protect the property and rights of Twitter or a third party, the safety of the public or any person, to prevent or stop illegal, unethical, or legally actionable activity, or to comply with the law*”<sup>36</sup>. (effective as of May 2007 until 18 November 2009). Concerns were expressed on the little expectation of privacy an anonymous poster appears to enjoy<sup>37</sup>. Eventhough the above privacy policy has been amended, the concerns still remain. The current privacy policy states that Twitter may disclosure user information if they believe “*it is reasonable necessary to comply with a law, regulation or legal request; to protect the safety of any person; to address fraud, security or technical issues; or to protect Twitter’s rights and property*”<sup>38</sup>.

It is obvious that the new privacy statement is more like rephrasing of the old one. We observe that the old express term that “*information might be disclosed even to private parties*” is omitted. Rather the new policy does not include any indication of the parties to which Twitter may reveal users’ private information of users. Thus, it leaves the possibility open that personal data may be given to *anyone* (public authorities, private third parties), shall the rights of Twitter be considered as threatened. The conditions on disclosure are wide and vague, absent any classification of rights which deserve protection or of the kind or extent of insults,

---

36. <[http://twitter.com/tos\\_archive/privacy\\_1](http://twitter.com/tos_archive/privacy_1)> (accessed 07/05/2011).

37. Tumbridge James, “Twitter: who’s really there?”, *Journal of Intellectual Property Law and Practice*, 2010, vol. 5, no. 2, p. 117 (available at <<http://jiplp.oxfordjournals.org>>, accessed 14/02/2011).

38. <<http://twitter.com/privacy>>.

illegal activities against third parties' rights. Insults against third parties via Twitter inevitably can be regarded by Twitter as threatening its own right or property.

In a recent case, the South Tyneside Council said that Twitter had released information entailed to identify a Twitter user on libel claims<sup>39</sup>. However, it is worth noting that Twitter has been praised for trying to fight US orders, which mandated personal user information to be handed out to authorities, without previously informing the subjects of the personal data so that they defend their case in court<sup>40</sup>.

## 6. Attempting to reconcile the conflicting rights

'If there be time to expose through discussion the falsehood  
or fallacies, to avert the evil by processes of education, the remedy  
to be applied is more speech, not enforced silence'

Whitney v. California<sup>41</sup>

Online speech as expressed in blogs has increasingly been at the center of judicial and public criticism as violating other protected rights, as the right to reputation and honor. Unanimous is the request for an effective way to safeguard free speech online and protect the rights of individuals. Law enforcement appears to be probably a solution. Thus, it does not prove to be totally effective in the absence of harmonized state provisions and with regard to the technical nature of online reality. It is doubtful whether a decision or order issued by a court in State A shall be willingly and effectively enforced by authorities or ISPs of State B<sup>42</sup>, where anonymity or free speech is more vigorously protected. Matters of *jurisdiction and applicable law* inevitable are brought forward.

### i. Injunctions

In addition, once a rumor or news is uploaded on the Web, it is multiplied in no time by propagating sites. After publication in various electronic media, courts seem to be powerless to undo what initially has been done. That was the case of a

39. BBC, 'South Tyneside Council 'gets Twitter data' in blog case', 30 May 2011, available at <<http://www.bbc.co.uk/news/uk-england-tyne-13588284>>.

40. Ball James, "Give Twitter credit for trying to stand up to the courts – unlike others", Guardian, 30 May 2011, available at <<http://www.guardian.co.uk/commentisfree/2011/may/30/twitter-privacy-courts?intcmp=239>>.

41. *Whitney v. California*, 274 U.S. 357, 1927 available at <<http://supreme.justia.com/us/274/357/case.html>> (accessed 29/04/2011).

42. A characteristic case, where the US court denied to enforce a French Judgment as conflicting with First Amendment right to free speech is *LICRA v. Yahoo!*

famous English married footballer, who had succeeded in getting a super-injunction<sup>43</sup> in order to prevent being identified as having a relationship with a model. Despite the injunction, several Twitter users named him online. The footballer reacted by obtaining a High Court order against Twitter to reveal the users who disclosed his identity. As soon as the order against Twitter was announced, “tens of thousands of people began posting his name online, openly taunting the judiciary and making a mockery of the legal system”<sup>44</sup>. It was estimated that 75.000 Twitter users posted his name. In addition, the footballer was publicly named by a Parliament Member -who enjoys parliamentary privilege to break the court order - during his speech, stating that with about 75,000 people having named that specific footballer, it would be obviously impracticable to imprison them all<sup>45</sup>. However, the Court suggested that the injunctions or other measures cannot be considered futile. When asking for the super injunction<sup>46</sup>, the judge stated that the need to protect privacy by e.g. preventing repetition by the press, still justifies an injunction even where the information is already in the public domain, or reproduced by social electronic media including Twitter.

In *CBT v. News Group Newspapers Ltd*, the Court decided that the above injunction should continue irrespective of the fact that thousands of people had identified the footballer and the model including a Parliament Member. It was concluded that the purpose of the injunction was not to preserve a secret but to prevent intrusion and harassment. Despite the fact that the injunction had not protected the claimant online, it would still be effective to protect him from any harassment by the print media<sup>47</sup>. So, it is obvious that enforcing injunctions against those who publish private information is difficult. The above was a case of protection of privacy. Likewise, in defamation/ libel cases once an offensive posting is submitted online, it is doubtful whether it can be deleted or whether an injunc-

---

43. “Super injunctions or else ‘gagging orders’ amongst press, prevent news organizations from revealing the identities of those involved in legal disputes, or even reporting the fact that reporting restrictions have been imposed in the first place”, Aliusman Samira, “Case Comment - Interim injunctions (super injunctions) – right to respect for private and family right”, *Coventry Law Journal*, 2011, 16 (1), 64-66.

44. Evans Martin, “Newspaper publishes name of footballer with gagging order”, *The Telegraph*, available at <<http://www.telegraph.co.uk/technology/twitter/8529609/Newspaper-publishes-name-of-footballer-with-gagging-order.html>>.

45. MSN News, “MP names player with gagging order”, 23/05/2011, available at <<http://news.uk.msn.com/uk/articles.aspx?cp-documentid=157738672>>.

46. *TSE v. News Group Newspapers Ltd*, [2011] EWHC 1308 (QB), Available at <<http://www.westlaw.co.uk>>.

47. *CTB News Group Newspaper Limited*, [2011] EWHC 1334 (QB) Date: 23/05/2011, available at <<http://www.westlaw.co.uk>>.

tion can be enforceable. Technology by means of cache pages, online archives etc. deprives the subject involved of an effective right to be forgotten.

## **ii. General obligation to monitor on Intermediary Service Providers (ISPs)?**

Another suggestion would be to impose obligations on ISPs. However, ISPs – at least on EU level- are unwilling to be granted with a general obligation to monitor, which would be accompanied with liability in case they failed to successfully do so<sup>48</sup>. They could be regarded as editors exercising editorial control. In addition, it would also come in contrast with the provisions of the E-commerce Directive.

Article 15 of the E-commerce Directive (2000/31/EC) indicates that “Member States shall not impose general obligations on providers, -when providing the services covered by articles 12, 13, 14- to monitor the information which they transmit or store, nor a general information actively to seek facts or circumstances indicating illegal activity”. However, according to article 12(3), 13(2), 14(3) of the Directive, courts or administrative authorities of a State can require service providers to terminate or prevent an infringement. In relation to hosting, Member States can establish procedures governing the removal or access to information.

In *L'oreal v. e-Bay* case, the issue of a general obligation to monitor was considered. *L'oreal*<sup>49</sup> tried to issue an injunction against *e-Bay* to prevent trademark infringement in the future. E-Bay argued that the injunction should be specific. A general injunction would have amounted to an unacceptable general obligation to monitor. The High Court faced the legal problem of whether the actual knowledge of an infringement for the purpose of article 14 of the E-commerce Directive refers only to the past or present and does not concern future infringements. “The judge was not satisfied this was *acte clair*”<sup>50</sup> and asked for a preliminary ruling. According to the principle of “notice and takedown” (article 14 of 2001/31/EC), the access provider has to take action and remove the content or disable access to illegal information upon *obtaining actual knowledge of the illegal activity*, or

48. In US jurisdiction, CDA par. 230 excludes ISPs from any tort liability.

49. *L'oreal S.A., Lancome Parfums ET Beaute, Laboratoire Garnier L' Oreal UK Ltd v. eBay International AG, eBay Europe S.A.R.L., eBay (UK) Limited, Stephen Potts, Tracy Ratchford, Marie Ormsby, James Clarke, Joanna Clarke, Glen Fox, Rukhsana BI*, Case No: HC07C01978, High Court of Justice Chancery Division 22 May 2009 [2009] EWHC 1094 (Ch) 2009 WL 1403418, Before: The Hon Mr Justice Arnold, Date: 22 May 2009, available at <<http://www.westlaw.co.uk>>.

50. McMahon Brian, “Imposing an obligation on Information Society service providers”, Computer and Telecommunications Law Review, 2011, available at <<http://www.westlaw.co.uk>>.

illegal information or awareness of facts or circumstances from which the illegal information or activity is apparent.

Considering the issue whether a court can issue an injunction against an intermediary and trying to find the balance between article 11 of 2004/48/EC<sup>51</sup> and 15 of 2001/30/EC, the advocate<sup>52</sup> came to the conclusion that there can be injunctions which prevent the continuation of the same or similar infringement in the future. However, the intermediary must be aware of what duty is imposed on him, which must not be equal to a general obligation to monitor. "An appropriate limit for the scope of injunctions may be that of a double requirement for identity", which means that the infringement and the infringer must be the same and known. A general obligation to monitor is seen by the advocate as an impossible, disproportionate or illegal duty<sup>53</sup>. So in case where there is no actual knowledge of an infringement and infringer, the general injunction is disproportionate. Besides the above, a general obligation to monitor by ISPs might result in over-monitoring activities, such as over-blocking or filtering at a disproportionate rate<sup>54</sup>. It must be noted that in case of blogs the filtering systems would scan all content

---

51. Article 11 of the enforcement directive 2004/ 48 indicates that "Member states shall also ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right".

52. Opinion of advocate general jääskinen delivered on 9 December 2010 (1) Case C324/09, available at <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62009C0324:EN:HTML>>.

53. "What is crucial, of course, is that the intermediary can know with certainty what is required from him, and that the injunction does not impose impossible, disproportionate or illegal duties like a general obligation of monitoring." Opinion of advocate general jääskinen delivered on 9 December 2010.

54. In the case of "SABAM v. Tiscali S.A. (Scarlet)", the District Court of Brussels stated that directive 2000/31 does not affect the power of the judge granting injunctive relief and does not limit the measures to be taken against the provider. In addition, it was concluded that the development of effective technical surveillance instruments is not precluded. The injunctive relief did not require Scarlet to monitor its network, but merely ordering a solution by means of a technical instrument aimed at blocking and filtering of certain information. So, according to the court there was no issue of violation of article 15 of the E-commerce directive. However, after a request for preliminary ruling by the court of appeal, the Advocate General suggested that a national law which mandates that ISP installs filtering systems to monitor all communications for unlimited period must be precluded. See Hughes J., Mady F., Bourrouilhou, English Translation of Sabam v. S.A. Tiscali (Scarlet), District Court of Brussels, 27 June 2009, available at <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1027954](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1027954)> and The IT Law Community, "ISPs, filtering and file sharing: advocate general's opinion published", 14 April 2011, available at <<http://www.scl.org/site.aspx?i=ne20418>>.

data online. Content data is protected by much stricter law provisions. Attention must also be given to Recital 46 of the E-commerce Directive which indicates that the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level.

However, according to article 12(3), 13(2), 14(3) of the E-commerce Directive the courts or administrative authorities of a State can require service providers to terminate or prevent an infringement. In relation to hosting, Member states can establish procedures governing the removal or access to information. In order for the ISPs to abide by the above rules, they have developed reporting mechanisms. The user can report any defamatory statement, and it can be removed by the service provider without any need to identify the blogger<sup>55</sup>.

In USA, the ISPs are expressly excluded from tort liability even if they control their content online. *InhZeran*<sup>56</sup> the court stated that the purpose of the Communications Decency Act par. 230 and the immunity of ISPs from tort liability was 'to encourage service providers to self-regulate the dissemination of offensive material over their services'. Congress has recognized that the specter of tort liability in an area of such prolific speech would have an obvious **chilling effect** and enacted par. 230 to remove the disincentives to self-regulation created by the *Stratton Oakmont* decision. In *Stratton Oakmont Inc. v. Prodigy Services Company* (1995)<sup>57</sup>, the Court concluded that the network provider PRODIGY was indeed a publisher – thus subject to stricter liability. Prodigy was considered a publisher by the Court, since it was exercising *editorial control* over the content posted on bulletin boards, and it presented itself *publicly* as controlling the content. Editorial control was utilized by the use of a *software screening program* which scanned bulletin boards for offensive language and by an *emergency delete function*.

### **iii. Self-regulation, self- help remedies**

Despite the above mentioned hardships in controlling Internet activity, net must not be seen as a virtual unregulated world where people's conduct is 'un-prin-

---

55. Sotiropoulos V., Blog's anonymity problem and the possibilities to overcome it, *Nomiki Epi-theorisi*, 36/ 2009, p. 24 (in Greek).

56. *Zeran v. American Online Incorporated*, 129 F. 3d 327 (4<sup>th</sup> Cir. 1997) available at <<http://caselaw.findlaw.com/us-4th-circuit/1075207.html>> (accessed on 29/04/2011).

57. *Stratton Oakmont Inc. v. Prodigy Services Company*, 1995 WL 805178 (N.Y. Supreme Court 1995), available at <<http://www.citmedialaw.org/sites/citmedialaw.org/files/1995-05-24-Prodigy%20Opinion.txt>> (Prodigy operated a computer network with at least 2 million subscribers, who could publish comments on the network's bulletin boards).



cipled'<sup>58</sup>. Those supporting cyber-anarchy indicate that Internet is a completely new system, where traditional offline laws do not apply. However, online and offline realities are interrelated, since Internet is just a new means both of communication and performance of offline activities. But even if it is seen as a new public place, it is not independent from the offline world; rather it tends to gradually substitute it. Thus, the principles of offline democratic world have to be applied thereon<sup>59</sup>.

Self-regulation and self-help remedies arise as a plausible solution to online defamation/ libel, offensive language disputes. As Mitrou Lilian indicates on the net codes of conduct comprise the most traditional form of self-regulation<sup>60</sup>. Codes of conduct mutually accepted and respected by bloggers shall be adopted. Since 2007, the operator of the blog [elawyer.blogspot.com](http://elawyer.blogspot.com) V.Sotiropoulos has already proposed a Blogger's Code of Conduct, where he has included a wide range of the most controversial issues regarding blogs such as anonymity (article 6), use of personal data, and confidentiality of communications<sup>61</sup>. Of course, even the adoption of codes of conducts does not solve all problems and questions are brought forward such as whether mutual acceptance of the rules is going to be achieved, which territory they are going to be applied (considering the borderless nature of online world).

Besides codes of conducts, in the online world the offended party is capable of and must be encouraged to engage in a form of online counterspeech<sup>62</sup> in order to exercise his right to respond to a libelous posting and present his own aspect of the story. Counterspeech is more plausible online and on blogs, where there is no strict editorial control as in the traditional press. So, everyone with a modem and a computer has the opportunity to publicly defend himself. Counter, speech has already been considered by US courts as a 'very powerful form of judicial relief' (*Cahill v Doe*)<sup>63</sup> and a first self-help remedy (*Gertz v. R. Welch*). The victim of a

---

58. Stratilatis K., Self-governance in the culture of online communication, in Self-governance, (Law and Society in 21<sup>st</sup> Century), Sakkoulas, Athens- Thessaloniki, 2005 (in Greek).

59. Kofinis, 2007.

60. Mitrou Lilian, Self-governance in cyberspace, in Self-Governance (Law and Society in 21<sup>st</sup> century), Sakkoulas, Athens- Thessaloniki 2005 (in Greek).

61. Sotiropoulos V., "Blogger's code of conduct", 20 March 2007, available at <[http://elawyer.blogspot.com/2007/03/blog-post\\_6732.html](http://elawyer.blogspot.com/2007/03/blog-post_6732.html)> and 'Explanation of the code of conduct', 21 March 2007, available at <[http://elawyer.blogspot.com/2007/03/blog-post\\_21.html](http://elawyer.blogspot.com/2007/03/blog-post_21.html)>.

62. Lieberman J.M., "Defamed by a blogger: Legal protections, self-regulation and other failures", Journal of Law, Technology and Policy, p. 343, 2006.

63. *Doe v. Cahill*, Supreme Court of the State of Delaware, October 5, 2005 available at <[https://www.eff.org/files/filenode/Doe\\_v\\_Cahill/doe\\_v\\_cahill\\_decision.pdf](https://www.eff.org/files/filenode/Doe_v_Cahill/doe_v_cahill_decision.pdf)>.

defamation case shall use available opportunities to 'contradict the lie or correct the error and thereby to minimize its adverse impact on reputation' (*Gertz v. R. Welch*). The nature of the Internet offers an existing opportunity, which allows for quick response to defamatory statements on the same site or blog, before the same audience, and 'the plaintiff can thereby easily correct any misstatements or falsehoods...and generally set the record straight' (*Cahill v Doe*, 2005).

#### *iv. Meta-public figures*

According to US law, public officials seeking damages for libel against their official conduct bear the burden to prove actual malice on the part of the defendant. Actual malice is defined as: "with knowledge that it was false or with reckless disregard of whether it was false or not"<sup>64</sup>. In Europe, a public figure is said to have greater endurance to criticism and comments<sup>65</sup>.

It is interesting to examine the defense of M. Brocks against whom libel suits were filed by Suarez Corp<sup>66</sup>. The case was settled, but the introduction of 'meta-public figures'<sup>67</sup> by Brocks' lawyers attracts legal attention. Brocks' side argued that the plaintiffs (an electronic postal service) had assumed an enhanced risk

64. *New York Times Co v. Sullivan*, 376 U.S. 254 (1964) Supreme Court, available at <[http://www.law.cornell.edu/supct/html/historics/USSC\\_CR\\_0376\\_0254\\_ZO.html](http://www.law.cornell.edu/supct/html/historics/USSC_CR_0376_0254_ZO.html)>.

65. "En premier lieu, s'agissant de l'objet des propos incriminés, la Cour rappelle que les limites de la critique admissible à l'égard d'un homme politique, visé en cette qualité, sont plus larges qu'à l'égard d'un simple particulier: à la différence du second, le premier s'expose inévitablement et consciemment à un contrôle attentif de ses faits et gestes, tant par les journalistes que par la masse des citoyens ; il doit, par conséquent, montrer *une plus grande tolérance* (*Lingens c. Autriche*, arrêt du 8 juillet 1986, série A no 103, p. 26, § 42). Ce principe ne s'applique pas uniquement dans le cas de l'homme politique mais s'étend à toute personne pouvant être qualifiée de personnage public, à savoir celle qui, *par ses actes* (voir, en ce sens, *Krone Verlag GmbH & Co. KG c. Autriche*, no 34315/96, § 37, 26 février 2002; *News Verlags GmbH & Co. KG c. Autriche*, no 31457/96, § 54, CEDH 2000-I) ou sa position même (*Verlagsgruppe News GmbH c. Autriche* (no 2), no 10520/02, § 36, 14 décembre 2006) entre dans la sphère de l'arène publique.", *Affaire I Avgi publishing and Press Agency S.A. & Karis c. Greece*, Application no. 15909/06, available at <<http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Avgi%2015909/06&sessionid=77659027&skin=hudoc-en>>.

66. *Suarez Corp. v. Meeks*, Civil No 267513, (Ohio C.P., Cuyahoga Country settled Aug. 1994). It is reported to be the first 'blogger' case, although the concept and software of a blog did not exist at that time. Robinson P. Eric, *Lawsuits against bloggers: MLRC's data on blog suits*, available at <<http://www.medialaw.org>>.

67. Rosenoer Jonathan, *Cyber law: the law of the Internet*, Springer -Verlag New York, Inc., 1997, p. 110.

of comment and criticism by voluntarily choosing the net as the medium of their communications for their business activities. In addition, 'they have ample ability to rebut criticism...Unlike traditional communications media where editors and news directors control who says what, the Internet provides plaintiffs with unfettered access to its mass audiences'<sup>68</sup>. As a result, posting online makes a person or a business more of a public figure and thus he has to prove actual malice of the defendant. In *Gertz v. Robert Welch* was held that the first remedy of a victim of defamation is self-help – using the available opportunities to contradict the lie. Public officials and public figures "usually enjoy significantly greater access to the channels of effective communication and, hence, have a more realistic opportunity to counteract false statements than private individuals normally enjoy"<sup>69</sup>. The Court states that the communication media are entitled to act on the assumption that public figures have voluntarily exposed themselves to increased risk of injury from defamatory falsehood concerning them. No such assumption is justified with respect to a private individual. Not all individuals shall be considered as public personalities for all aspects of their lives. It would be preferable, according to the Supreme Court in *Gertz*, to reduce the public figure question to a more meaningful context by looking to the nature and extent of an individual's participation in the particular controversy giving rise to defamation/ offense language.

Nowadays, technology is said to have challenged and changed the nature of 'public figures'. All that is needed is a modem and a keyboard to "thrust [oneself] into the vortex' of public debate online"<sup>70</sup> and to count as a public figure. Most Internet users create profiles in multiple networks, like Facebook, Twitter, LinkedIn, MySpace, Google+ etc. They have the opportunity to make their profiles private, or public. They upload photos of personal moments, vacation and friends, and offer a variety of information on their everyday activities, either private or public, their relationships, their favorite music, the cinema they went and the restaurant they ate at. So, people online voluntarily place themselves in the public spotlight and expose themselves to an increased risk of injury from defamatory statements. The -more or less- voluntary exposure to the public renders personality relative -not absolute- protection<sup>71</sup>. As a matter of fact, a person must endure personality infringe-

---

68. Meeks Defend Fund, Jacking in from 'The Rest of the Story' Port, available at <<http://cyberwire.com/mdf/closure.94.11.07.html>>.

69. *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974) decided 25 June 1974, available at: <<http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=418&invol=323>>.

70. Godwin Mike, *Cyber Rights- Defending free speech in the digital age*, Massachusetts Institute of Technology, 2003, p. 99.

71. Chatzikostas K., *Insults to honor out of justified interest*, Sakkoulas, 2005, p. 91 (in Greek).

ments in accordance with the way of life he chose<sup>72</sup>. So, if someone participates in a public demonstration or watches a football game or reveals private information about himself<sup>73</sup>, he accepts the fact that he is 'followed' –to use Twitter terms- by others and that he may become the center of discussion, comments and criticism, which he must tolerate. However, whether an insulted user has invited attention and comment cannot be inferred merely from the fact that he possesses a computer, modem and accesses the web and his profile. Rather it depends on the kind of online activities and public dialogue the user engages, the kind of profile he maintains (the terms of use he has accepted, the settings he has chosen), the subjects he addresses and the nature and extent of his participation in particular controversies.

Besides the voluntary exposure online, another factor which differentiates Internet users from traditional private figures, is the fact that Internet facilitates better, faster and easier access to communications media and social networks, thus, enabling the offended party to instantly rebut criticism and to engage in counter-speech. The offended has the ability to define the time, content, audience, and host of his response, something which grants greater and faster relief online. As has already been noted, Internet does not allow for anything uploaded to be forgotten, either it is a defamatory posting or a response by the offended party. So, the statement correcting the errors will be accessible to everyone who may search on the particular dispute.

In the above context, an acknowledgement of a meta-public figure can be justified. The offended party should be more tolerant to defamatory statements in the sense that -before seeking court orders- they should try to utilize self-help remedies. The insulted has the means to defend himself online, and to make an attempt to settle things non-judicially. But in addition, the offending party has to abide either by traditional rules or code of conducts, show respect for his other e-citizens, and be willing even to retract false or defamatory postings.

## Conclusion

Free speech is one of the most valuable rights in a democracy, a way to defend one's rights, to report the falsehoods of governments. It promotes prolific debates and contributes to progress by the exchange of ideas and thoughts. Bloggers claim freedom of speech and expression privileges. However, protection of free expression is not absolute. Limits are drawn, where other rights are violated, such as the right to reputation: "Who stole my purse steals trash...But he that filches me my good name, robs me of that which not enriches him, and makes me poor

---

72. Karakostas I., *Personality and the press*, Sakkoulas, 2000, p. 58 (in Greek).

73. Karakostas I. *ibid.* p. 58.

indeed”<sup>74</sup>. Regulators around the world attempt to balance the involved rights. However, regulation or case-law is not harmonized. Rather they mostly depend on the legal tradition and practices of each country. In any case, a chilling-effect on free speech and the submission of SLAPPs (Strategic Lawsuit Against Public Participation) must be avoided. The situation becomes more complicated due to the borderless nature of the web. Self-regulation and self-help remedies by means of an attempt to deal with a dispute via interactive civilized speech, or to abide by mutually approved codes of conduct are welcomed. And as Tim O’Reilly<sup>75</sup> states in his proposed code of conduct for bloggers:

*“We celebrate the blogosphere because it embraces  
frank and open conversation. But frankness does not  
have to mean lack of civility. We present this Blogger  
Code of Conduct in hopes that it helps create a culture  
that encourages both personal expression and  
constructive conversation”*

## References

### Articles

Aliusman Samira, “Case comment - interim injunctions (super injunctions) – right to respect for private and family right”, *Coventry Law Journal*, 2011, 16 (1), 64-66.

Ball J., “Give Twitter credit for trying to stand up to the courts – unlike others”, *Guardian*, 30 May 2011, available at <<http://www.guardian.co.uk/commentisfree/2011/may/30/twitter-privacy-courts?intcmp=239>>.

BBC, ‘South Tyneside Council ‘gets Twitter data’ in blog case’, 30 May 2011, available at <<http://www.bbc.co.uk/news/uk-england-tyne-13588284>>.

Ciolly A., Bloggers as public figures, 16 B.U. Pub. Int. L.J. 255, 2006-2007.

Evans M., “Newspaper publishes name of footballer with gagging order”, *The Telegraph*, available at <<http://www.telegraph.co.uk/technology/twitter/8529609/Newspaper-publishes-name-of-footballer-with-gagging-order.html>>.

74. Shakespeare, *Othello* Act 3, scene 3, as quoted in Troiano Melissa, “The new journalism? why traditional defamation laws should apply to internet blogs”, *The American University Law Reviews*, vol. 55, issue 5, (June 2006), p. 1451-1452.

75. <<http://radar.oreilly.com/archives/2007/04/draft-bloggers-1.html>>.

Gibb Frances, Ruling on NightJack author Richard Horton kills blogger anonymity, *The Times*, June 17, 2009, <[http://technology.timesonline.co.uk/tol/news/tech\\_and\\_web/the\\_web/article6509677.ece](http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article6509677.ece)>.

Kanakis Ant., Blogs: freedom or not?, 10/04/2011, [www.aixmi.gr](http://www.aixmi.gr).

Kathimerini, "Creation of law drafting committee on blogs", 05-08-2011, available at <[http://portal.kathimerini.gr/4dcgi/\\_w\\_articles\\_kathbreak\\_1\\_05/08/2011\\_401345](http://portal.kathimerini.gr/4dcgi/_w_articles_kathbreak_1_05/08/2011_401345)> (in Greek).

Kofinis St., Participation in Information Society as a new constitutional right, DIMEE 4, 2007 (in Greek).

Liebman J.M., Defamed by a blogger: Legal protections, self-regulation and other failures, *Journal of Law, Technology and Policy*, 343, 2006.

McMahon B., "Imposing an obligation on Information Society service providers", *Computer and Telecommunications Law Review*, 2011, available at <[westlaw.co.uk](http://westlaw.co.uk)>.

Meeks Defend Fund, Jacking in from 'The Rest of the Story' Port, available at <<http://cyberwire.com/mdf/closure.94.11.07.html>>.

MSN News, "MP names player with gagging order", 23/05/2011, available at <<http://news.uk.msn.com/uk/articles.aspx?cp-documentid=157738672>>.

Ott Stephan (Dr), Die Impressumpflcht nach § 5 TMG / § 55 RStV, available at <<http://www.linksandlaw.info/Impressumpflcht-Notwendige-Angaben.html>>.

Pagkalos Th., Information and press in the era of blogs, 23/04/2011, *Kathimerini Newspaper*, <[http://news.kathimerini.gr/4dcgi/\\_w\\_articles\\_columns\\_3\\_23/04/2011\\_439985](http://news.kathimerini.gr/4dcgi/_w_articles_columns_3_23/04/2011_439985)> (in Greek).

Ribstein E. L., From bricks to pajamas: the law and economics of amateur journalism, 48 *WM & Mary L. Review* 185, 187, 2006.

Robinson P. E., Lawsuits against bloggers: MLRC's data on blog suits, available at <<http://www.medialaw.org>>.

Sotiropoulos V., "Blogger's code of conduct", 20 March 2007, available at <[http://elawyer.blogspot.com/2007/03/blog-post\\_6732.html](http://elawyer.blogspot.com/2007/03/blog-post_6732.html)>.

Sotiropoulos V., Blog's anonymity problem and the possibilities to overcome it, *Nomiki Epitehorisi*, 36, 2009 (in Greek).

Sotiropoulos V., 'Explanation of the code of conduct', 21 March 2007, available at <[http://elawyer.blogspot.com/2007/03/blog-post\\_21.html](http://elawyer.blogspot.com/2007/03/blog-post_21.html)> (in Greek).

Stathopoulos M., Use of personal data and the fight among freedoms of the data holders and freedoms of the data subjects, Nomiko Vima, January 2000, vol. 1 (in Greek).

The IT Law Community, "ISPs, filtering and file sharing: advocate general's opinion published", 14 April 2011, available at <<http://www.scl.org/site.aspx?i=ne20418>>.

Troiano M., "The new journalism? why traditional defamation laws should apply to internet blogs", The American University Law Reviews, vol. 55, issue 5, June 2006.

Tumbridge J., Twitter: who's really there?, Journal of Intellectual Property Law and Practice, 2010, vol. 5, no. 2, p. 117, available at <<http://jiplp.oxfordjournals.org>>.

### **Books**

Chatzikostas K., Insults to honor out of justified interest, Sakkoulas, 2005 in Greek.

Dagtoglou, Human and social rights, Sakkoulas, 2005 in Greek.

Fotiadou Alk., Balancing the freedom of speech, Sakkoulas, 2006 in Greek.

Godwin M., Cyber Rights- defending free speech in the digital age, Massachusetts Institute of Technology, 2003 in Greek.

Karakostas I., Personality and the press, Sakkoulas, 2000 in Greek.

Kastanas H., Internet and the protection of privacy and freedom of expression: in query of smart provisions, in New Technology and Constitutional Rights (Law and Society in the 21<sup>st</sup> century), 2004 in Greek.

Mitrou L., Self-governance in cyberspace, in Self-Governance (Law and Society in 21<sup>st</sup> century), Sakkoulas, Athens- Thessaloniki, 2005.

Stratilatis K., Self-governance in the culture of online communication, in Self-governance, (Law and Society in 21<sup>st</sup> Century), Sakkoulas, Athens- Thessaloniki, 2005.

Rosenoer J., Cyber law: the law of the Internet, Springer -Verlag New York, Inc., 1997.

### **Case Law**

Affaire I Avgi publishing and Press Agency S.A. & Karis c. Greece, Application no. 15909/06, available at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Avgi%20|%2015909/06&sessionId=77659027&skin=hudoc-en>.

CTB News Group Newspaper Limited, [2011] EWHC 1334 (QB) Date: 23/05/2011, available at <<http://www.westlaw.co.uk>>.

*Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974) decided 25 June 1974, available at <<http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=418&invol=323>>.

*Hughes J., Mady F., Bourrouilh, English Translation of Sabam v. S.A. Tiscali (Scarlet)*, District Court of Brussels, 27 June 2009, available at <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1027954](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1027954)>.

*L' Oreal S.A., Lancome Parfums ET Beaute, Laboratoire Garnier L' Oreal UK ltd v. eBay International AG, eBay Europe S.A.R.L., eBay (UK) Limited, Stephen Potts, Tracy Ratchford, Marie Ormsby, James Clarke, Joanna Clarke, Glen Fox, Rukhsana BI*, Case No: HC07C01978, High Court of Justice Chancery Division 22 May 2009 [2009] EWHC 1094 (Ch) 2009 WL 1403418, Before: The Hon Mr Justice Arnold, Date: 22 May 2009, available at <<http://www.westlaw.co.uk>>.

*Maire d' Orleans Serge G. vs Antoine B.- blogueur*, Serge G. Cour d'appel D'Orléans Chambre civile Arrêt du 22 mars 2010 Antoine B. / Serge G. available at <[http://www.legalis.net/spip.php?page=jurisprudence-decision&id\\_article=2919](http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2919)>.

*Maire d' Orleans Serge G. vs Antoine B.- blogueur* Tribunal de grande instance d'Orléans Ordonnance de référé 08 octobre 2008 Serge G. / Antoine B. available at <[http://www.legalis.net/?page=jurisprudence-decision&id\\_article=2912](http://www.legalis.net/?page=jurisprudence-decision&id_article=2912)>.

*New York Times Co v. Sullivan*, 376 U.S. 254 (1964) Supreme Court, available at <[http://www.law.cornell.edu/supct/html/historics/USSC\\_CR\\_0376\\_0254\\_ZO.html](http://www.law.cornell.edu/supct/html/historics/USSC_CR_0376_0254_ZO.html)>.

Opinion of advocate general jääskinen delivered on 9 December 2010 (1) Case C324/09, available at <[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=C\\_ELEX:62009C0324:EN:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=C_ELEX:62009C0324:EN:HTML)>.

*Stratton Oakmont Inc. v. Prodigy Services Company*, 1995 WL 805178 (N.Y. Supreme Court 1995), available at <<http://www.citmedialaw.org/sites/citmedialaw.org/files/1995-05-24-Prodigy%20Opinion.txt>>.

*Suarez Corp. v. Meeks*, Civil No 267513, (Ohio C.P., Cuyahoga Country settled Aug. 1994).

*The author of a blog v. Times Newspaper Limited* [2009] EWHC 1358 (QB).

*TSE v. News Group Newspapers Ltd*, [2011] EWHC 1308 (QB), Available at <<http://www.westlaw.co.uk>>.

*Whitney v. California*, 274 U.S. 357, 1927 available at <<http://supreme.justia.com/us/274/357/case.html>> (accessed 29/04/2011).

*Zeran v. American Online Incorporated*, 129 F. 3d 327 (4<sup>th</sup> Cir. 1997) available at <http://caselaw.findlaw.com/us-4th-circuit/1075207.html> (accessed on 29/04/2011).



# Self-determination and information privacy: a plotinian virtue ethics approach

---

---

Giannis Stamatellos

---

---

## Introduction

The emergence of advanced mobile technology, social networking and sophisticated ICT surveillance tools leads to a philosophical reconsideration of our social life and ethical values. The Internet is the new *cyberagora*, where the netizens of a *cyberpolis* exchange goods and ideas in *cyberspace*. Internet users experience a *cyberlife* oscillating among the private, the public and the global sphere. The ontological unity of the self is pluralized in digital representations of our selves in virtual environments. The *cyberself* is a new digital identity involved in novel forms of ethical practice and human selfhood.

The ethical issue of privacy lies at the core of computer ethics and cyber ethics inquiry. In the information economy sensitive data and personal information are the most valuable commodity. Personal data are used and freely distributed for economic or security reasons and in some cases unverified, without the knowledge of the individuals and the groups involved in the procedures. The extensive and unrestricted use of personal information poses a serious threat to the user's right of privacy not only at the level of a user's data integrity and security but also at the level of a user's identity and freedom.

In contemporary studies, the problem of information privacy (DeCew, 2006) has been closely related to informational self-determination and the claim or the ability of individuals and groups to determine for themselves when, how, and what kind of information about themselves is shared with or communicated to others (Westin, 1967). The normative approach of informational self-determination focuses on the action of moral agency and the evaluation of ethical decision. However, a self-directed virtue ethics approach of self-determination has not been acknowledged in modern discussions.

Plotinus' notion of human freedom and self-determination is toward this direction: to be self-determined means to take steps towards our inner-self and to discover our own principles of thought that govern our intellectual freedom and autonomy. In this paper I shall argue that Plotinus' approach of self-determination could be enlightening in computer ethics and cyber ethics inquiries of information privacy and human freedom. Plotinus' notion of self-determination moves

the emphasis of information privacy from the nature of the action and the possible consequences of our moral decisions to the quality of the self and the virtue of the moral agent. A virtuous moral action is initially based before the action in the character-based quality of the agent who performs the action in voluntariness, self-knowledge and intellectual autonomy.

## Information Privacy

The problem of privacy as a social value has attracted the interest of scientists, legislators and philosophers. As Alan Westin (1967) observes in the opening words of his influential book *Privacy and Freedom*: “few values so fundamental to society have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists”. Modern studies usually distinguish between *descriptive notions* of privacy (i.e. a description of what is protected as private) and *normative notions* of privacy (i.e. defending the value or the right to privacy and the extent to which it should be protected) (DeCew, 2006). However, divergent views have been expressed about the moral and legal right of privacy. The most important of these views have been discussed and summarized by DeCew (1997 and 2006).

On the one hand, critics of the privacy right have questioned the importance of privacy. As Thomson (1975) states, “it is a useful heuristic device in the case of any purported violation of the right to privacy to ask whether or not the act is a violation of any other right, and if not whether the act *really* violates the right at all” (313-314). Moreover, excessive forms of privacy such as *anonymity* may protect the guilty, cover deception and fraud and so may appear dangerous to personal life and social stability. An example of this is the feminist critique of the use of privacy to cover up abuse and control of women (MacKinnon, 1989 Bottis 2000).

On the other hand, supporters of privacy accept the importance of privacy as a moral value that paves the way to human freedom and social stability. It has been argued that privacy should be defended on the grounds of control over our personal information (Parent, 1983). Privacy has also been regarded as essential for human dignity (Bloustein, 1964), intimacy (Innes, 1992; Gerstein, 1984), human freedom and independence (DeCew, 2006). Finally, privacy is considered as a social value with moral significance, fundamental to individual integrity and personal autonomy (Bloustein, 1964), as well as to the self-development of the individual in interpersonal relationships such as love, friendship and trust (Fried, 1970; Gerstein, 1978).

Privacy has also been analyzed as an *intrinsic* value (i.e. privacy desired for its own sake) and an *instrumental* value (i.e. privacy desired as a means to other ends)

(Tavani, 2007). While privacy has been considered as an instrumental value that serves the intercultural core value of security (Moor, 2001), it has also been regarded as an intrinsic value necessary to achieve important human ends, such as trust and friendship (Fried, 1997). Privacy is an intrinsic value that promotes democracy and social goods (Regan, 1995). However, it has been argued that privacy should not necessarily be regarded as a universal value of equal importance and significance for all cultures and societies (Westin, 1967).

Alan Westin (1967) considers privacy as a human value related to four human rights: *solitude* (i.e. the right to be alone), *anonymity* (i.e. the right to have no public identity), *intimacy* (i.e. the right to act in private) and *reserve* (i.e. the right to control your personal information). Herman Tavani (2007) further distinguishes among three definitions of privacy: *accessibility privacy* (i.e. privacy defined as the freedom from unwarranted intrusion into one's physical space), *decisional privacy* (i.e. privacy defined as freedom from interference in one's personal affairs, choices and decisions), *information privacy* (i.e. privacy defined as control over the flow of personal information). The right of privacy is also related to different forms of personal protection and identification, such as *territorial privacy* (i.e. protects domestic, professional, civil and recreational environments); *location privacy* (i.e. privacy of an individual's location); *bodily privacy* (i.e. respect of an individual's body); *personal privacy* (i.e. protects an individual's personal identity); *communication privacy* (i.e. protects an individual's personal communication); *information privacy* (i.e. determination of an individual's use and dissemination of personal data) (Stamatellos, 2007).

Information privacy is closely related to the rise of modern technology and it is noteworthy that this issue has been emphasized since the late 19<sup>th</sup> century. Warren and Brandeis in their 1890 paper 'The Right of Privacy' emphasized the importance of privacy protection against such new technological inventions and practices as the snapshot photography used in newspaper journalism, especially without the knowledge of the individuals photographed. Warren and Brandeis (1890) observed a moral problem in the rise of new media technologies that cause not only a threat to the private life of the individual but also to the morality of society as a whole. With Warren and Brandeis, the right of privacy as the *right to be alone* is developed into the right of information privacy, that is, *the right to one's own personality* (DeCew, 2006).

The problem of information privacy in the digital age has been particularly discussed and evaluated in terms of the *amount* of the gathered personal information, the *speed* of transmission of personal information, the *duration* of time that personal information is retained and the *kind* of personal information that can be transferred (Tavani, 2007) as well as the accessibility, availability and storage

of personal information in social networks and distributed databases (Stamatellos, 2007). ICT methods of information privacy violation may include *information intrusion* (i.e. wrongful entry, seizing, or acquiring possession of property that belongs to another person), *information misuse* (i.e. illegal use of information for unauthorized purposes), *information interception* (i.e. unauthorized access to private information or communication), *information matching* (i.e. information combined, compared and collected from two or more electronic sources) (Stamatellos, 2007).

The ICT involved in information privacy threats may include surveillance technologies such as *database surveillance* (e.g. black list databases, database mismanagement, data theft), *internet surveillance* (e.g. 'cookies' that track user's web preferences), *video surveillance* (e.g. CCTV cameras in public places), *satellite surveillance* (e.g. GPS technology), *mobile surveillance* (e.g. 3G mobiles using high definition video and pictures), *card surveillance* (e.g. smart cards, e-passports, biometric technologies) (Stamatellos, 2007). As Jerry Kang (1998) observes, various surveillance technologies, especially those applied in cyber-activities, present a serious threat to information privacy. Another noteworthy case is the problem of information privacy threats in advanced genetic research and database medical records. Judith DeCew (2004) discussed this issue in her paper 'Privacy and Policy for Genetic Research', emphasizing the importance of protecting the privacy of sensitive medical and genetic information by suggesting a hybrid synthesis of governmental guidelines and corporate self-regulation.

## Plotinus on Self-determination

Plotinus' discussion of self-determination is mainly exposed in the first part of his *Ennead VI.8 On the voluntary and the wish of the One*. Particularly, in the first seven chapters of the treatise Plotinus exposes his arguments on the nature of human freedom. Plotinus uses the term *autexousios* in order to denote one's own power to be self-governed and self-determined. Another key Enneadic term for the analysis of human freedom and self-determination is the notion of *eph' h min* (i.e. what is in our power or what depends on us). Plotinus criticizes the Stoic and Aristotelian notions of *eph' h min*: an action depends on us not only through rational deliberation of and decision about the facts related to the action but also through normative knowledge of what we ought to do or what we ought not to do in the situation. A virtuous action is not carried out for the sake of external situational facts but for the sake of the inner perfection of the soul. Whereas Aristotle conceives human freedom as related to the problem of choice and contingency, Plotinus conceives human freedom as related to the true freedom of the self (Leroux, 1996). Human freedom is not necessarily defined by voluntary choice but is manifested in the virtuous life of the soul (VI.8.1-7).

Plotinus wonders: “Is there anything in our power?” “What do we mean when we speak of ‘something being in our power’ and what are we trying to find out?” (VI.8.1). We could falsely regard our actions as *voluntary* if we consider that we are not obliged to act, while we could falsely regard our actions as *knowledgeable* if we follow uncritically the path of reason. In both cases, an action may *not* depend on us and, if it does not depend on us, it is not free and ethical. An action depends on us only if the agent establishes himself as a self-determined principle (III.1; VI.8.3.20-26). Hence Plotinus distinguishes between *internal determinations* (i.e. what depends on us) and *external determinations* (i.e. what is not dependent on us) (Remes, 2006; Eliasson, 2008). Something depends on us when we are purely self-determined by internal conditions. However, self-determination alone is not sufficient nor is it an unqualified positive term. An “empty” self-determination might incline the soul to what is better but also to what is worse (III.2.4) and may cause individuation and fragmentation to the self (IV.8.8). The *eph’ hēmin* is not a “mere word” (III.1.7.15), but signifies the intellectual autonomy and virtue of the soul. The virtuous moral agent acts autonomously in inward determination and not in heteronomous outward actions determined by external factors and conditions (VI.8.6.19-23).

In modern Plotinian scholarship, divergent interpretations arise from the notion of self-determination in the *Enneads*, oscillating between an action-centered interpretation (i.e. self-determination refers to the agent’s power of choice) and a self-centered interpretation (i.e. self-determination refers to the human agent itself and the perfection of the soul).

Graeser (1972) interprets Plotinus’ notion of self-determination in the light of the Kantian distinction between the empirical self and the non-empirical self. Whereas the quality of our actions (*praxis*) is dependent on our own power and our empirical self as the real subject of choice (the case of *eph’ h min*), man’s liberty is not determined by the power of choice - in Aristotelian or Stoic terminology - but by our self-determination of the non-empirical self (i.e. the case of *autexousios*).

However, as Remes (2007) warns us, a Kantian approach to autonomy may be problematic for ancient literature. A modern conception of autonomy carries within itself a Kantian and post-Kantian conception of self-legislation and individualization (i.e. a moral action is carried by an individual who binds himself to universal rules) (180). Whereas the Greek notion of autonomy (*autonomos* = living by one’s laws) was used both for states and persons, “treatises on moral autonomy are hard to find in ancient literature” (179). However, this gap in the literature does not mean “that ancient philosophers did not have opinions on what

it means to be an agent, when an action is free or what makes an agent responsible for his actions" (179).

Leroux (1990) interprets Plotinus' notion of self-determination in relation to the concept of *eph' hemin* as having the connotation of a faculty describing either the *quality of action* (*eph' hēmin*) or the *agent himself* (to *eph' hēmin*). Erik Eliasson (2008) further distinguishes between an inclusive notion of *eph' hemin* (i.e. the moral action has its origins in the agent) and an exclusive notion of *eph' hemin* (i.e. the moral action has its origins in rational decisions and judgments not necessarily determined by the agent). For Plotinus, mere voluntariness and awareness of an action is not enough for an action to be dependent on us. An action depends on "an agent if and only if it happens because of a wish coming through the thought and contemplation of virtue" (205). As Remes (2007) states: for Plotinus "truth, goodness and even freedom exist independently of human activities" (181). The action of a free and self-determined moral agent reflects his true inner freedom and the perfection of the soul.

Plotinus suggests three conditions for a free and virtuous action: an action must be (1) voluntary (i.e. we should not be forced to act), (2) conscious (i.e. we should have knowledge of what we are doing) and (3) self-determined (i.e. we should be masters of ourselves) (Eliasson, 2008). With the third condition of self-determination, Plotinus moves the emphasis of a moral action from action to the self, from outward activity to inner activity, from *praxis* to the *psyche*. A noble action should not be based on the *action itself* in a duty-based ethical perspective, but on the *quality of the agent* in a virtue ethics perspective. Plotinus stresses the fact that there is no practical or outward action that is purely dependent on us: "in practical actions self-determination and being in our power does not refer to practice and outward activity but to the inner activity of virtue itself, that is, its thought and contemplation" (VI.8.6.20-22). Being in our own power does not belong to the realm of action but to that of the intellect at rest from actions (VI.8.5.35-37). Only virtue itself – as an inner-self intellectual activity – purifies and frees the soul: virtue has "no master" and so intellectualizes the soul through its own self-recognition, self-constitution and self-determination. (VI.8.5.30-37).

### **Plotinian self-determination and information privacy**

In modern discussions of information privacy the importance of self-determination has been explicitly identified. Alan Westin's (1967) definition of privacy puts a strong emphasis on self-determination: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (7). Moreover, David Flaherty relates privacy to the right of informational control: individuals have the

right to exercise the same control over their personal data as they exercise over themselves (Flaherty, 1989). The right of self-determination is regarded as integral to a free society: as Richard James Severson (1997) states, “we must learn to think of personal data as an extension of the self and treat it with the same respect we would a living individual. To do otherwise runs the risk of undermining the privacy that makes self-determination possible.” (67-68). The right of informational self-determination has been also defined with reference to natural and legal persons and the right of individuals and groups to control the release of their personal information as well as to know the processes through which their personal data is communicated (Lopez, Furnell, Katsika and Patel, 2008).

Nevertheless, a conflation of privacy with freedom and autonomy has been questioned and criticized (Wacks, 2010). However, Rafael Capurro (2010) had argued that in the light of the Kantian criticism of Aristotelian metaphysics, contemporary biotechnology and information and communication technologies bring the new challenge to reconsider the Kantian moral subject as a unique metaphysical quality of dignity and autonomy. The new cyberspace of artificial agency blurs the boundaries between the human and the natural realm and leads to a philosophical reflection on ethics, law and practical policies. An intercultural perspective is also fruitful in the understanding of privacy and the self in relation to human freedom and autonomy in cyberspace and the mass media (Capurro, 2006). It has been successfully maintained that a concept of the self as empowered to determine the life of an individual is requisite for acting autonomously in a moral and social perspective of privacy (Kupfer, 1987).

Plotinus’ notion of self-determination is towards this direction: it is related to human freedom, intellectual autonomy and independence of the soul as well as connected to a self-centered virtue ethics and moral psychology. In a recent paper, I have supported the view that Plotinus’ self-directed virtue ethics of intellectual autonomy and self-determination are relevant to cyber ethics and, in particular, the character-based moral act of moral selfhood applicable in computer education and netizenship (Stamatellos, 2011).

It has to be noted, however, that a systematic treatment of the problem of privacy cannot be found in ancient literature. Some first attempts towards a philosophical discussion of the notion of privacy in terms of a distinction between private life and public life may be sporadically identified in ancient thinkers. For instance, Democritus underlined the importance of measure and self-control in the serenity both of the private (*idie*) and the public (*ksine*) life (fr. 3). In his *Republic*, Plato offers an analogy between the soul (*psyche*) and the city-state (*polis*): the inner structural form of the city-state is analogous to the individual soul. As the human *psyche* consists of three parts (i.e. desire, spirit, reason), equally the *polis* consists

of three classes (i.e. producers, guardians, rulers) (Wright, 2009). However, for Plato there is no clear-cut distinction between the private and the public sphere. Political life is an extension and fulfillment of the life of the individual activated in the community. Aristotle moved a step further in his *Politics* and attempted a comparison between the public sphere of the *polis* and the domestic sphere of the household (*oikia*), i.e. the basic social unit of the *polis* (Nagle, 2006).

Plotinus follows Plato and describes the human *psyche* as a “double city”: the higher self as a city above, self-ordered and self-organized, and the lower self as a city below, “set in order by the powers above” (IV.4.17.30 ff.). Plotinus conceives two aspects of the self: the intelligible inner-self and the corporeal outer-self (Remes, 2007). Plotinus’ inward turn towards the self (*epistrophē pros heauton*) is a novel direction in Platonic ontology and metaphysics. Plotinus’ notion of the inner self plays a significant role in the philosophical development of the notion of the self as an inner and private space. As Remes (2007) notes, it moves from Plato’s shared intellectual vision of the eternal Forms, to an inner contemplation of an eternal realm in our selves, and then to St Augustine’s private inner space of the soul contemplating God, to John Locke’s private inner space of an individual subject differentiated from the outside world (p. 6, n. 21). However, in Plotinus, as Remes (2007) observes, “the inner realm is still only private. If the turn is accomplished with success, the inward turn will ultimately reveal objective realities and infallible knowledge” (6-7). Plotinus conceives the self not as a private realm of subjectivity, fragmentation and individuality but as an intelligible unified self where the ‘I’ discovers the ‘We’.

The moral and philosophical significance of privacy in one’s personality and inner self has been stressed by Shoeman (1984) while Robert Gerstein (1978) traces back the notion of intimacy and privacy to Plotinus’ ecstatic experience of the inner self. However, Plotinus’ notion of self-determination is not an ecstatic, ascetic, individualistic or even egotistic self-directed morale of disclosure. The issue of regarding privacy in terms of disclosure has already been underlined by Westin (1967) in terms of modern technologies. The Plotinian self is not disclosed nor detached from the public sphere (Stern-Gillet, 2009; Remes, 2006). The Plotinian wise is not isolated, unfriendly or inconsiderate but renders to “his friends all that he renders to himself, and so will be the best of friends as well as remaining intelligent” (I.4.15.23-25); nor does he aim to have advantage over “private persons” (*idioton*) (II.9.9.1-5). The private life should not be regarded in terms of a cloistered life or as detachment from the public sphere: “for one must not [live] in a *private manner*, but like a great combatant be in a state to ward off fortune’s blows” (I.4.8.24-26). The term *idiotikos* in this passage is usually translated as ‘untrained’ (Armstrong, 1966; McGroarty, 2007), “languid” (modern Greek *nothros*: Kalligas, 1994) or ‘in a commonplace way’ (Sleeman, 1980). My sugges-



tion is that the term *idiotikos* in I.4.8.24-26 also entails a criticism of the private life as disclosed or alienated life (other uses of entry *idiotikos* in LSJ). Whereas the private life could be related to an 'untrained' person, Plotinus' aim is not so much to criticize an untrained way of living but a passive or detached way of living - probably related to some Stoic or Gnostic ethical trends of his era - contrasted to an active, virtuous and courageous way of life followed consciously by the wise.

For Plotinus, to determine our selves is not to alienate or dehumanize the self but to free the mind from heteronomous affections, passions and reasons. If self-determination is used as disclosure, it leads to dehumanization and alienation. If self-determination is used for self-knowledge, self-control and self-constitution, it leads to the unity, perfection and virtue of the soul. Virtue leads to the soul's self-development, self-recognition and self-knowledge. We have to *become what we are*: to "sculpt the statue of ourselves" and care for our soul in a continuous process of self-improvement through the *purification of virtue* (I.6.9). Virtue purifies the soul in its noetic ascent (I.4) and leads the soul to the understanding of the others through contemplation of our inner self (VI.9.11).

Plotinus' notion of self-determination could also be seen as a motivational rather than a cognitive approach. As Deci and Ryan (1990) support, in a motivational approach to self, intrinsic motivation is experienced as truly self-determined, that is, what one wants to do, with a sense of freedom of choice, not controlled even by internalized rules that one experiences as coercive. As Plotinus puts it: "for everything is a voluntary act which we do without being forced to and with knowledge [of what we are doing], and in power which we are also competed to do" (VI.8.1.32-34). Whereas the voluntariness and knowledge of an action can be undermined by external conditions, it is only our knowledge of self-determination that makes an action dependent on us. An involuntary action leads away from the good and towards the compulsory (VI.8.4). What depends on us is not a simple expression but signifies our self-determination, ethical autonomy and freedom (III.1.7). A person who acts in accordance with virtue should be guided by internal and autonomous self-determinations and not by external and heteronomous predeterminations (VI.8.6).

Plotinus' virtue ethics is a self-directed theory (Dillon, 1996; Plass, 1982; Smith, 1999; Stern-Gillet, 2009). In this virtue ethics approach of information privacy, self-determination is relevant to online communities and social networking, where the act of self-determination is a necessary prerequisite and demand by the online users (Stamatellos, 2011). A virtue ethics information privacy act should be protected not only by privacy policies or online commands and rules but also by encouraging user's education, self-development, and self-awareness (Grodzinsky, 2001). As Castoriadis has supported, an autonomous

society is not only self-instituted but also promotes and enforces self-awareness and responsibility in its members (Tasis, 2007). People who are educated in autonomy and self-justice become self-aware of their own values and rights (Castoriadis, 2000).

Thus, the importance of Plotinian self-determination lies not in the action alone but in the ethical quality of the moral agent who performs the action. For Plotinus, the best actions derive from ourselves who act in accordance to our own thinking and will and not by not being hindered or by being allowed; a “breathing space” (anapneusosi) to decide our actions cannot justify the nobility of our actions (III.1.10.10-15). Freedom is not that which the others permit us but how we free ourselves through our will and through thinking without predeterminations. An act of self-determination privacy in cyber ethics should also include a virtue ethics self-directed perspective: privacy should derive from the users themselves as virtuous agents who act in voluntariness, knowledge of their actions and informational self-determination.

## Conclusion

Plotinus’ notion of self-determination makes us rethink the importance of a computer agent’s privacy, intellectual autonomy and freedom in the information society. We have to reevaluate the importance of our privacy in the information age not in terms of disclosure but in terms of freedom to determine our own life and self. To be self-determined should not be merely an “ability” or “claim” of an individual to determine *when*, *how*, and *what kind* of personal information is shared with others. Informational self-determination must primarily focus on the ethical quality of the individuals and groups to know *why* information about themselves *should* or *should not* be shared with or communicated to others. Plotinus puts an emphasis not on moral action but on the ethical virtue of the self who performs the action. Virtuous actions derive from ourselves when we *know* ourselves and *act* in accordance to our own thinking and will and *not* because we are hindered or allowed to act. This form of self-awareness enforces the unity, dignity and knowledge of the individuals both in private and public life. The universality of the Plotinian self and the self-deterministic notion of information privacy reestablishes the moral subject in an intellectual autonomy and virtue necessary in the multi-divergent global sphere of the *cyberself*.

## References

- Armstrong, A. H. (1966-1988), *Plotinus*, Greek text with English translation in 7 vols. Cambridge, Mass.: Heinemann.
- Bloustein, E. (1964), "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser", *New York University Law Review* 39: 962-1007.
- Bottis, M. (2000) The problem of founding the right to information of a patient and the right to abortion on the right of privacy, *Critical Review of Legal Theory and Practice*, 2000/1, Sakkoulas, pp. 179-194 (in Greek).
- Capurro, R. (2006), "Privacy: An Intercultural Perspective", online at <http://www.capurro.de/privacy.html> accessed 22.12.2010, originally published in *Ethics and Information Technology* (2005) 7: 37-47.
- Capurro, R. (2010), "Towards a Comparative Theory of Agents", online at <http://www.capurro.de/agents.html> accessed 22.12.2010.
- Castoriadis, C. (2000), *The Talks in Greece*, Athens: Ypsilon.
- DeCew, J. (1997), *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Ithaca: Cornell University Press.
- DeCew, J. (2004), "Privacy and Policy for Genetic Research", *Ethics and Information Technology*, 6, 1: 5-14.
- DeCew, J. (2006), "Privacy", online at <http://plato.stanford.edu/entries/privacy/> accessed 20.3.2011.
- Deci, E. L., and Ryan, R. M. (1990), "A motivational approach to self: integration in personality", *Nebraska Symposium On Motivation*, 38: 237-288.
- Dillon, J. (1996), "An ethic for the late antique sage", in Gerson, L. P., *The Cambridge companion to Plotinus*, Cambridge: Cambridge University Press, 315-335.
- Eliasson, E. (2008), *The Notion of That Which Depends On Us in Plotinus and Its Background*, Brill.
- Flaherty, D. (1989), *Protecting privacy in surveillance societies*. Chapel Hill, U.S.: The University of North Carolina Press.
- Fried, C. (1970), *An Anatomy of Values*, Cambridge: Harvard University Press.
- Fried, C. (1997), "Privacy: A Rational Context", in Ermann, M. D., Williams, M. B., and Gutierrez, C., *Computer, Ethics and Society* New York: Oxford University Press.
- Graeser, A. (1972), *Plotinus and the Stoics: A Preliminary Study*, Brill.

Grodzinsky, F. (2001), "The Practitioner from Within: Revisiting the Virtues" in Spinello, A. R., and Tavani, T. H., *Readings in Cyberethics*, Jones and Bartlett Publishers, 580-591.

Inness, J. (1992), *Privacy, Intimacy and Isolation*, Oxford: Oxford University Press.

Kalligas, P. (1994), *Plotinus' Ennead I: Ancient Greek text, translation and commentary*, Athens: Centre of Edition of Ancient Greek Authors.

Kang, J. (1998), "Information Privacy in Cyberspace Transactions", *Stanford Law Review*, 50, 4: 1193-1294.

Kupfer, J. (1987), "Privacy, Autonomy, and Self-Concept", *American Philosophical Quarterly*, 24, 1: 81-89.

Leroux, G. (1990), *Traité sur la liberté et la volonté de l'Un*. [VI.8(39)] Paris: Vrin.

Leroux, G. (1996), "Human freedom in the thought of Plotinus", in Gerson, L. P., *The Cambridge companion to Plotinus*, Cambridge: Cambridge University Press, pp. 292-314.

Lopez, J., Furnell, S., Katsikas, S. and Patel, A. (2008), *Securing Information and Communications Systems: Principles, Technologies, and Applications*, Artech House Publishers.

MacKinnon, C. (1989), *Toward a Feminist Theory of the State*, Cambridge: Harvard University Press.

McGroarty, K. (2007), *Plotinus on Eudaimonia. A Commentary on Ennead I.4*. Oxford: Oxford University Press.

Moor, J. H. (2001), "Reason, Relativity, and Responsibility in Computer Ethics", in

Spinello, A. R., and Tavani, T. H. *Readings in Cyberethics*, Jones and Bartlett Publishers, 36-54.

Nagle, D. B. (2006), *The Household as the Foundation of Aristotle's Polis*, Cambridge: Cambridge University Press.

Parent, W. (1983), "Privacy, Morality and the Law", *Philosophy and Public Affairs* 12: 269-88.

Plass, P., (1982), "Plotinus' ethical theory", *Illinois Classical Studies*, 7, 2: 241-259.

Regan, P. M. (1995), *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill: The University of North Carolina Press.

- Remes, P. (2006), "Plotinus' ethics of disinterested interest", *Journal of the History of Philosophy*, 44: 1-23.
- Remes, P. (2007), *Plotinus on Self: The Philosophy of the 'We'*, Cambridge: Cambridge University Press.
- Schoeman, F., (1984), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge: Cambridge University Press.
- Severson, R. J. (1997), *The principles of information ethics*, M. E. Sharpe: Armonk, N.Y.
- Sleeman, J. H. (1980), *Lexicon Plotiniaum*, Leiden: E. J. Brill.
- Smith, A., (1999), "The significance of practical ethics for Plotinus", in Cleary, J. J., *Traditions of Platonism: Essays in Honor of John Dillon*, Aldershot, 227-236.
- Stamatellos, G. (2007), *Computer Ethics: A Global Perspective*. Jones and Bartlett Publishers.
- Stamatellos, G. (2011), "Computer Ethics and Neoplatonic Virtue: A Reconsideration of Cyberethics in the Light of Plotinus' Ethical Theory", *International Journal of Cyber Ethics in Education*, 1, 1: 1-11.
- Stern-Gillet, S. (2009), "Dual Selfhood and Self-Perfection in the *Enneads*", *Epoché: A Journal for the History of Philosophy*, 13, 2: 331-345.
- Tasis, Th., (2007), *Castoriadis: A Philosophy of Autonomy*, Eurasia.
- Tavani, T. H. (2007), *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*, Wiley.
- Thomson, J. (1975), "The Right to Privacy", *Philosophy and Public Affairs* 4: 295-314.
- Wacks, R. (2010), *Privacy: A Very Short Introduction*, Oxford: Oxford University Press.
- Warren, S. and Brandeis, L. (1890), "The Right to Privacy," *Harvard Law Review* 4: 193-220.
- Westin, A. (1967), *Privacy and Freedom*, New York: Atheneum.
- Wright, M. R. (2009), *Introducing Greek Philosophy*. Acumen Publishing.

# **Towards an updated EU Enforcement Directive?**

## **Selected topics and problems**

---

---

**Irini Stamatoudi**

---

---

### **I. Introduction**

Intellectual property (IP) infringements have taken considerable dimensions during the last years and have become a real threat both for right holders and consumers. A variety of international and European Union instruments have dealt with this issue, but in a rather sporadic and incomplete manner in the sense that they are usually rather vague and general in nature, they leave considerable discretion to States, each one of them deals with different intellectual property rights and most of them were drafted when digital infringements were still at a premature stage<sup>1</sup>. The EU Enforcement Directive<sup>2</sup> was the first European Union instrument which dealt with the issue of IP enforcement in a more structured and organized manner providing Member States with a TRIPs Plus Element. Lately many initiatives have taken place in the area of IP enforcement<sup>3</sup>. However, the

- 
1. For the situation today see for example <<http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/OECD-FullReport.pdf>>; <[http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Building%20a%20Digital%20Economy%20-%20TERA\(1\).pdf](http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Building%20a%20Digital%20Economy%20-%20TERA(1).pdf)>.
  2. Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights, OJ L157/16, 30.04.2004.
  3. See indicatively, at European Union level:
    - the relevant provisions of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ No L 178/1 of 17.07.2000) and Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ No L 167/10 of 22.6.2001);
    - Council Regulation (EC) No 1383/2003 of 22 July 2003 concerning customs action against goods suspected of infringing certain intellectual property rights and the measures to be taken against goods found to have infringed such rights;
    - amended Proposal for a Directive of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights (COM (2006) 168 final of 26.4.2006);
    - Commission Strategy for the Enforcement of Intellectual Property Rights in Third Countries of 2005 and to the Commission Staff Working Document 'IPR Enforcement Report 2009' (OJ No C129 of 26.5.2005);

- 
- draft Report of the Committee on Legal Affairs on enhancing the enforcement of intellectual property rights in the internal Market, 13.1.2010, (2009/2178(INI));
  - Resolution of the European Parliament on defining a new digital agenda for Europe: from i2010 to digital.eu, 5.5.2010, (2009/2225(INI));
  - European Parliament, Resolution of 22 September 2010 on enforcement of intellectual property rights in the internal market (2009/2178(INI)), A7-0175/2010.
  - draft Opinion of the Committee on Industry, Research and Energy for the Committee on Legal Affairs (European Parliament) on enforcement of intellectual property rights in the internal market, 29.01.2010, (2009/2178(INI));
  - draft Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Legal Affairs (European Parliament) on enhancing the enforcement of intellectual property rights in the internal market, 5.02.2010, (2009/2178(INI));
  - Council Resolution of 1 March 2010 on the enforcement of intellectual property rights in the internal market (OJ C 56/01);
  - Commission Communication of 11 September 2009 on enhancing the enforcement of intellectual property rights in the internal market (COM (2009) 467 final);
  - Resolution of 25 September 2008 on a comprehensive European anti-counterfeiting and anti-piracy plan including the European network for administrative cooperation referred to in it with a view to ensuring rapid exchanges of information and mutual assistance among the authorities engaged in the field of the enforcement of intellectual property rights (OJ C 253/1);
  - Conclusions of 20 November 2008 on the development of legal offers of online cultural and creative content and the prevention and combating of piracy in the digital environment (OJ L 195/16);
  - Commission Communication of 16 July 2008: 'An industrial property rights strategy for Europe', COM (2008)465 final; Commission Communication: 'Enhancing the enforcement of intellectual property rights in the internal market', COM(2009) 467 final.
  - the Telecom Package (Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (OJ L 337/37);
  - Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121/37);
  - Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view of reinforcing the fight against serious crime (OJ L 63/1);
  - Conclusions of 24 September 2009 on "Making the internal market work better" (Council Document 13024/09);
  - Commission Recommendation 2009/524/EC of 29 June 2009 on measures to improve the functioning of the single market (OJ L 176/17);
  - the European Observatory on Counterfeiting and Piracy;
  - proposals for the review of the Brussels I Regulation (Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 12/1)); see, for example, Report from the Commission to

EU Enforcement Directive continues to be the most significant legal instrument in the area. In a recent assessment of the Directive on the basis of article 18, the European Commission came to the conclusion that it is difficult to assess the effectiveness of the Directive as this has been transposed late in many Member States although the expiry of the deadline for the implementation of the Directive was 29 April 2006<sup>4</sup>. On top of it, a number of issues are pinpointed as being capable of improvement or change according to the requests/opinions by Member States, the industry and other stakeholders. One of these issues -perhaps the most important one- is the fact that this Directive falls short of dealing adequately with digital infringements, whilst its relation with other EU Directives cutting across relevant issues in this field is not without problems. On the basis of the above an updating of the Enforcement Directive has come on the EU agenda.

## II. Problem issues and open questions

### A. *Scope of protection*

The Directive relates to civil law measures concerning the enforcement of intellectual property rights. Criminal sanctions were dropped before the Directive's adoption and became the content of another draft directive<sup>5</sup>. This Directive presents a blend of civil law and civil law procedure, but by no means constitutes a reflection of a civil law tradition. It is rather a compromise between the civil law and the common law traditions or -even better- a collection (puzzle) of various procedures found in different Member States which were thought to be useful and effective with regard to enforcement (a best practices approach). What, also, needs to be kept in mind is that this Directive does not intend to harmonise

---

the European Parliament, the Council and the European Economic and Social Committee on the application of Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (COM(2009) 174 final);

- the setting up of ENISA: the European Network and Information Security Agency, working for the EU Institutions and Member States and dealing with security issues of the European Union (<http://www.enisa.europa.eu/about-enisa>).

*At international level:*

- The Anti-counterfeiting Trade Agreement (ACTA);

- the Advisory Committee on Enforcement (ACE) approved by the WIPO General Assembly at its 23rd September to 1st October 2002 session.

4. See Report on the enforcement of intellectual property rights (COM (2010) 779), and Analysis of the application of Directive 2004/48/EC on the enforcement of intellectual property rights in the Member States (SEC (2010) 1589).

5. Amended Proposal for a Directive of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights (COM (2006) 168 final of 26.4.2006).



the enforcement regime in all Member States in a uniform manner, since it only provides for minimum harmonization level, i.e. leaves Member States free to introduce (or retain) stricter provisions favourable to rightholders, if they so wish. This, however, has taken place in reality with regard to only few provisions in the Directive<sup>6</sup>. There are also several voluntary provisions that have not been implemented by some Member States<sup>7</sup>.

The Directive was meant to apply to any infringement of intellectual property rights whether these rights were provided for by European Union law or the law of the Member States<sup>8</sup>. This formed a rather flexible approach but, at the same time, it was open to multiple interpretations. Following a Member States' request the European Commission published a statement which contained a minimum list of the intellectual property rights that were covered by the Directive<sup>9</sup>. This statement clarified that amongst the rights covered by the Directive are copyright and related rights, the sui generis right of a database maker, rights of the creator

---

6. "One of the examples where some Member States have gone beyond the Directive's wording was the right of information (Article 8) which, according to the Directive, is limited to the activities carried out on a commercial scale if the request is not directed towards the infringer. A significant number of Member States (e.g. Denmark, Estonia, Greece, France, Lithuania, Slovak Republic) have gone beyond the 'commercial scale' requirement (of which there is no definition in the Directive) and introduced this measure for all infringements [...]. Another example where Member States have gone beyond the Directive's provisions was damages. As far as damages are concerned, most Member States did not specifically implement the Directive's provisions as they felt that their national laws already covered them sufficiently. However, as far as lump sum damages are concerned, some Member States (e.g. Austria, Belgium, Greece, Czech Republic, Lithuania, Poland, Romania, Slovenia) have moved beyond the Directive's provisions and introduced multiple damages awards. Such multiple (mostly double) awards are available for copyright (and rights related to copyright) infringements or for infringements committed in bad faith". European Commission Staff Working Document, "Analysis of the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights in the Member States Accompanying document to the Report from the Commission to the Council, the European Parliament and the European Social Committee on the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights" COM(2010) 779 final (Brussels, 22.12.2010 SEC(2010) 1589 final), p. 5.

7. "As an example, many Member States have opted for non-transposition of the alternative measures provided for in Article 12 of the Directive (e.g. Austria, Belgium, France, Luxembourg, the Netherlands, and Slovenia). Likewise, many Member States (e.g. Czech Republic, Greece, Hungary, Malta, and Poland) have opted for non-implementation of description orders (Article 7(1)), which are often available in criminal proceedings only", *op. cit.* p. 6.

8. Article 2(1).

9. Statement by the Commission concerning Article 2 of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights (2005/295/EC).

of the topographies of a semiconductor product, trademark rights, design rights, patent rights, including rights derived from supplementary protection certificates, geographical indications, utility model rights, plant variety rights and trade names in so far as these are protected as exclusive property rights in the national law of the Member State concerned.

Although this statement was considered to be helpful, it still did not clarify the area exhaustively. Questions remained as to domain names, trade secrets and know-how, appellations of origin and unfair competition law (in particular parasitic copies and other forms of commercial misbehavior). In a series of meetings that took place concerning issues of enforcement at the level of the European Council, many suggestions were made. One suggestion was to draft a new minimum list of intellectual property rights covered by the Directive. Another suggestion was to draft an exhaustive list of intellectual property rights covered by the Directive. These lists could either be in the preamble to the Directive (a non-exhaustive list is found there currently) or within the actual text of the Directive. However, reservations were made regarding the extension of the Directive's scope. Such an extension did not seem to be welcome by most Member States. As a whole, however, the fact that the European Union chose to have a legal instrument applicable to all intellectual property rights and not only to those covered by the *acquis communautaire* or Community rights alone was regarded as an important step forward with rather positive effects on the single market. This is so irrespective of the fact that the European Union was criticised in the past for such a holistic approach.

### ***B. Infringements on the Internet, intermediaries and issues pending***

The notion of an 'intermediary' is rather broad in the Directive aiming to cover any third party whose services are used to infringe an intellectual property right be it a transporter, intermediate trader or Internet platform. That means that it is irrelevant for the purposes of the Directive whether this person or entity is in direct contractual relationship with the infringer or not as well as whether s/he is in good faith when acting or not. In other words, the liability of the intermediary is also irrelevant for the purposes of the Directive in the sense that measures may also imposed on the intermediary as means to stop or prevent further infringements to which it contributes or facilitates<sup>10</sup>.

---

10. See I. Stamatoudi, "Data Protection, Secrecy of Communications and Copyright Protection. Conflicts and Convergences. The Example of *Promusicae v. Telefonica*" I. Stamatoudi (ed), Copyright Enforcement and the Internet, Information Law Series (B. Hugenholtz (general editor), Kluwer Law International, 2010, at 199. See also I. Stamatoudi, «Ethics, Reality and the Law: The Example of *Promusicae v. Telefonica* & *LSG v. TELE2*» [2010] 63 *Revue Hellénique de droit International* 921; I. Stamatoudi, «Ethics, Codes of Conduct and P2P», 3<sup>rd</sup> International Seminar on Information Law 2010, "An Information Law for the 21st Cen-

However, the fact that injunctions, for example, can be applied for and taken irrespective of the liability of internet service providers is not entirely clear in the Directive and merits perhaps further clarification<sup>11</sup>.

The Enforcement Directive does not provide for the liability (or non-liability) of internet service providers (and intermediaries in general). Its focus is rather on enforcement than liability. The E-Commerce Directive<sup>12</sup> is more specific on liability. ISPs are exempt from liability when they serve as a “mere conduit” (Article 12)<sup>13</sup>,

---

tury”, Ionian University, Corfu, 25-26 June 2010, Nomiki Vivliothiki, Athens, 2010, 476, and I. Stamatoudi «The role of Internet Service Providers. Ethics, Reality and the Law: The Example of *Promusicae v. Telefonica*», 8th International Conference, Computer Ethics: Philosophical Enquiry, Ionian University, Corfu, 26-28 June 2009, Nomiki Vivliothiki, Athens, 2009, 750 (ed. M. Bottis). See also J. Raynard, Intellectual Property Enforcement in Europe: Acquis and Future Plans, Intervention lors de la conférence organisée par le CEIPI dans le cadre du réseau EIPIN sur le thème «Constructing European IP: Achievements and New Perspectives», Strasbourg, European Parliament, 25 February 2011, Edward Elgar Publishing (in print); the conference organized by the Facultés Universitaires Saint Louis, the Université Libre de Bruxelles and the Université de Liège on «Quelles réponses juridiques au téléchargement d'oeuvre sur internet? Perspectives belges et européennes», Université Libre de Bruxelles, Bruxelles, 14 December 2010, Larcier (in print). See also Ch. Geiger, J. Raynard and C. Rodà, L'application de la directive du 29 avril 2004 relative au respect des droits de propriété intellectuelle dans les États Membres. Observations du CEIPI sur le rapport d'évaluation de la Commission européenne du 22 décembre 2010, <<http://www.ceipi.edu/index.php?id=8601>>.

11. Injunctions against intermediaries whose services are used by a third party to infringe copyright or related rights were already provided for in Article 8(3) of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001, p. 10).
12. Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178/1, 17.7.2000.
13. 1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
  - (a) does not initiate the transmission;
  - (b) does not select the receiver of the transmission; and
  - (c) does not select or modify the information contained in the transmission.
2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication net-

provide “temporary caching” (Article 13)<sup>14</sup> or host services (Article 14)<sup>15</sup>. In this latter case though, in order not to be liable they have to act expeditiously to remove or to disable access to the information as soon as they become aware or gain knowl-

---

work, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement.

14. Communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients of the service upon their request, on condition that:

- (a) the provider does not modify the information;
- (b) the provider complies with conditions on access to the information;
- (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
- (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
- (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement.

15. 1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

- (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

edge of illegal activity or information. In relation to mere conduit and caching the Directive also refers to the fact that it does not affect the possibility of Member States' judicial or administrative systems to require an ISP to terminate or prevent an infringement. In relation to hosting it is also added that it does not affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15 sums up that in all the aforementioned cases service providers have no obligation to monitor the information which they transmit or store or actively seek facts or circumstances indicating illegal activity. However, Member States may establish obligations on service providers to promptly inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements. That means that Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation<sup>16</sup>. In addition the Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care which can reasonably be expected from them, and which are specified by national law in order to detect and prevent certain types of illegal activities<sup>17</sup>.

Given the fact that ISPs provide to their customers access to the Internet, facilitate the exchange of protected material, host sites and servers and form the only basic and essential facility for any online communication, they can play a useful role in reducing infringements on Internet regardless of their liability.

The *right of information* may also be exercised in order to obtain information by internet service providers with regard to infringements committed on their networks and platforms including the identity of the persons engaging in illegal conduct. This right, however, may clash with privacy laws, i.e. the protection of personal data and the secrecy of communications<sup>18</sup>. At this point, a balance has to be struck between these rights as they both form fundamental rights recognized by

---

16. Recital 47 to the E-commerce Directive.

17. Recital 48 to the E-commerce Directive.

18. See for example the 2009 Study on Online Copyright Enforcement and Data Protection in Selected Member States (Hunton & Williams, Brussels, <[http://ec.europa.eu/internal\\_market/iprenforcement/docs/study-online-enforcement\\_en.pdf](http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf)>).

the Charter of Fundamental Rights of the European Union<sup>19</sup>. This has also been concluded in two rather recent judgments of the Court of Justice of the European Union, which in fact leave it up to Member States to find the appropriate solutions reflecting this balance<sup>20</sup>. We need, however, to admit that finding a solution is not an easy task since it refers to a politically heated issue, which touches on the sensitivities of all the parties and stakeholders concerned. In addition to that any national solutions chosen so far, such as for example the HADOPI system in France, the UK Digital Economy Act, the Code of Conduct for ISPs in the Netherlands, the Memorandum of Agreements concluded between rightholders and ISPs in Ireland or the recent laws in Italy and Spain, have not paid off so far in order for their results to be appreciated in substance<sup>21</sup>. That means that we need to wait a bit longer in order to appreciate the actual results or the effects of those initiatives.

From the above, it is clear that the Enforcement Directive is rather neutral when it comes to the liability of Internet Service Providers<sup>22</sup>. This is not the case with the E-Commerce Directive, which is more specific on this point. ISPs do not have a general monitoring obligation, but when they gain knowledge of the infringement duties arise. For this reason there is currently discussion as to which of the two legal instruments is more appropriate for accommodating an effective regime of combating piracy on the Internet and regulating the role of ISPs. Other legal instruments have also been proposed such as the Trade Mark Directive (I believe with little success since their scope is by definition limited).

Another issue is whether one can request information by intermediaries which they are not obliged to retain. There may be cases where the data required has either not been stored or by the time requested has been erased either because

---

19. Charter of Fundamental Rights of the European Union (2000/C 364/01), OJ C364, 18.12.2000, p. 1.

20. Judgment of 29 January 2008 in the case C-275/06 *Productores de Música de España (Promusicae) v. Telefónica de España SAU*; judgment of 19 February 2009 in the case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GMBH v. Tele2 Telecommunication GMBH*. See also the Scarlet case C-70/100 and the Netlog case C-360/10, which are currently pending before the CJEU.

21. For more national initiatives in this area see the site of the Hellenic Copyright Organisation <[www.opi.gr](http://www.opi.gr)>.

22. The issue of liability of ISPs is also discussed at WIPO level since at the end of March 2011 officials agreed to plan a meeting on internet service provider liability <[http://www.ip-watch.org/weblog/2011/04/04/wipo-slowly-advances-industrial-design-treaty-eyes-isip-liability-for-trademarks/?utm\\_source=monthly&utm\\_medium=email&utm\\_campaign=alerts](http://www.ip-watch.org/weblog/2011/04/04/wipo-slowly-advances-industrial-design-treaty-eyes-isip-liability-for-trademarks/?utm_source=monthly&utm_medium=email&utm_campaign=alerts)>.

ISPs have not retained it out of their free will or because they were obliged to erase it by privacy laws. There is European Union legislation which deals with data retention (data retention is dealt with at EU level only in the Data Retention Directive<sup>23</sup> and in the e-privacy Directive<sup>24</sup>) and which needs to be seen in conjunction and in conformity with any 'new regime' of enforcement in the area of infringements on Internet.

One easily notices that the plurality of regulations at EU level on topics, which cross each other create on occasions conflicts or clashes which cannot be sorted out easily. One more of them, is the issue of confidentiality. Confidentiality covers different information in different Member States. That means two things; Firstly, not all information, which will allow parties to pursue their rights or pursue their rights effectively, can be obtained. Secondly, even if such information is made available in one Member State, this does not mean that it can be used with no problems in other Member States. Concrete provisions on information which is or which is not confidential should be provided for in order for infringements to be combated effectively on Internet throughout the European Union.

### ***C. Collection of evidence and cross-border collection of evidence on the Internet***

Cross-border collection of evidence presents a general problem and not one relating only to infringements on Internet. However, we shall focus on the latter. Given the fact that sites may be established anywhere in the world and operate anywhere in the world, too, cross-border collection of evidence is necessary. This collection does not so much present problems with regard to the particular nature or kind of the information that needs to be gathered (as in other cases where you need for example to specify the exact character, location, reference numbers and contents of the requested documents, sometimes even the page numbers of the defendant's commercial records)<sup>25</sup>, but rather to the gathering itself from two

---

23. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54.

24. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.

25. See European Commission Staff Working Document, "Analysis of the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights in the Member States Accompanying document to the Report from the Commission to the Council, the European Parliament and the European Social Committee on the application of Directive 2004/48/EC of the European Parlia-

points of view. First, it is difficult to issue orders for the gathering of evidence abroad. Even if these orders are issued and they do not correspond to a known form of order abroad they cannot be executed. On top of everything even if they correspond to a relevant order abroad it is not certain again that this order will be executed, especially if it is considered to impinge on other rights such as the right of privacy. In cases of infringements on Internet on many cases data is required to prove that infringements are conducted on a commercial scale. Without this data it is difficult to prove the seriousness and extent of the infringement. Second, the evidence that may be collected in these cases (such as screenshots) does not carry a certain weight in all cases. Since screenshots reflect the situation in a particular moment in time, they are not always accepted by courts as full evidence or even if accepted it is in the courts' complete discretion as to how they shall assess it.

Various proposals have been made as to how this situation can be amended. An improvement of the rules on jurisdiction of the courts to issue provisional measures has been proposed as well as the provision of the ability to transform a measure granted by a foreign court into one known in the State, where this measure is intended to apply. The free circulation of measures ordered *ex parte* within the European Union has also been proposed. This is also an issue which is examined in the context of the upcoming revision of Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I Regulation)<sup>26</sup>.

Article 6(1) seems also to present some problems. According to it "if the right-holder has presented reasonably accessible evidence sufficient to support his claims and has, in substantiating those claims, specified evidence which lies in the control of the opposing party the competent judicial authority may order that the opposing party produce evidence under its control". The two issues which present problems, as these problems have been reported by various Member States, are the 'specified evidence' and the notion of 'control'. Given the flexibility of the wording, some national courts require very specific and accurate description as to the evidence required. For example, in order for bank accounts to be disclosed data should be made available to the court as to the banks at issue, the numbers of the accounts, the names on the accounts and so on. As it becomes apparent it is not easy for one to submit all this information. On top of it, the no-

---

ment and the Council of 29 April 2004 on the enforcement of intellectual property rights" COM(2010) 779 final (Brussels, 22.12.2010 SEC(2010) 1589 final), p. 9.

26. Also in relation to article 5(3) the question needs to be asked whether the restriction to local damage makes sense in an internet context where infringement of copyright material happens everywhere. The risk of limiting the provision to local damage only may result in endless fragmentation and an inability to enforce rights effectively.



tion of 'control' is not specified. It is not clear whether it only refers to evidence in the possession of the party that is required to disclose or also to evidence that this person can get hold of after reasonable search. The prevailing view seems to be the first one.

#### ***D. Infringements committed on a commercial scale***

The notion of commercial scale is another issue which is not properly harmonized in all Member States. A general definition is provided for in Recital 14 of the Directive according to which "*acts carried out on a commercial scale are those carried out for direct or indirect economic or commercial advantage; this would normally exclude acts carried out by end consumers acting in good faith*". Some Member States have provided for their own definitions (only few of them)<sup>27</sup>, which however differ. Some others have chosen to extend the measures (i.e. allow communication of banking, financial or commercial documents) provided for infringements committed on a commercial scale to other infringements, too. However, Member States do not seem to be positive for having a general harmonized definition of 'commercial scale' given the fact that their national systems have so far dealt with this issue adequately and have developed considerable jurisprudence in this respect.

### **III. Conclusions**

The enforcement Directive seems to have worked well so far with no substantial problems. This is so despite the fact that it constitutes a puzzle of good practices, some of them unknown to some Member States. However, one may argue that the Directive was transposed late into the laws of the Member States and actual practice and case law are not indicative as to what worked well and what did not work well so far. Greece forms a characteristic example in this respect since it is

---

27. E.g. Germany, Czech Republic, Romania, Slovenia. Italian scholars seem to conclude that «on a commercial scale» means «in the course of trade». The definition is often given by using the notion of «commercial purpose» and defining it as "purposes aimed at direct or indirect economic or commercial gain" or similar. Different e.g. Germany for copyright infringements ("number or severity of infringements"). European Commission Staff Working Document, "Analysis of the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights in the Member States Accompanying document to the Report from the Commission to the Council, the European Parliament and the European Social Committee on the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights" COM (2010) 779 final (Brussels, 22.12.2010 SEC(2010) 1589 final), p. 9.

only now that tries to align itself to the Directive's obligations regarding trademarks and patents. Copyright has been aligned properly and within the deadline.

Taking into account the various points that have been raised so far in the Commission's report, none of them seems to carry considerable weight -for the time being- in order for Member States to actually push forward the amendment/updating of the Directive apart from one; the role of intermediaries and in particular internet service providers concerning large scale intellectual property infringements on the Internet. However, a decision has to be made whether the enforcement Directive is the right instrument for accommodating such a provision. One also needs to take into account the fact that this issue is being currently discussed (or tackled) on other levels, too. One forum which currently holds informal discussions of this kind is the World Intellectual Property Organisation.

At European Union level, this issue has been indirectly dealt with in the Telecoms package<sup>28</sup>, whilst the e-commerce Directive and the trademark Directive form alternative options. Very recently on 24 May 2011 the European Commission has

---

28. In the Telecoms Package it was decided that no measures restricting end-users' access to the Internet may be taken unless they are appropriate, proportionate and necessary within a democratic society and never without a prior, fair and impartial procedure that includes the right to be heard and respects the presumption of innocence and the right to privacy (Amendment 46 (ex 138) of the Telecom Package, which amends Art. 1 para. 3a) of Directive 2002/22/EC of the European Parliament and of the Council of 7 Mar. 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) '3a. Measures taken by Member States regarding end-users' access to or use of services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law. Any of these measures regarding end-users' access to or use of service and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of presumption of innocence and the right to privacy. A prior fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to an effective and timely judicial review shall be guaranteed'. The Telecom Package: (Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and intercon-

announced a formal strategy concerning intellectual property rights, which aims at modernising the existing legal framework in which IPRs operate<sup>29</sup>. According to the European Commission's press release "this will benefit the EU's growth and competitiveness which is delivered through the single market"<sup>30</sup>. IP actions and/or concerns are provided for in the Digital Agenda for Europe<sup>31</sup>, where seven actions relate directly or indirectly to IP rights (including the revision of the enforcement directive and the e-commerce directive), in Europe 2020 Strategy<sup>32</sup>, in the Annual Growth Survey 2011<sup>33</sup>, in the Single Market Act<sup>34</sup> and in the Innovation Union<sup>35</sup>. It is very likely that the European Union will try to be more concrete in involving ISPs into the combat of piracy on Internet. This however will be done not by reason of the fact that it believes that ISPs should incur some kind of liability, but because there is no other stakeholder that can offer effective services in that particular field. Also any measures taken will be within the liability framework it has provided for ISPs in the E-commerce Directive. In the meantime, a number of national initiatives leading to legal or soft law solutions have taken place following the general trend towards the effective protection of rightholders and the limitation of the ISPs' 'asylum'<sup>36</sup>. The fact is that the longer

---

nection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services (OJ L 337/37)).

29. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions a single market for intellectual property rights boosting creativity and innovation to provide economic growth, high quality jobs and first class products and services in Europe, 24.5.2011, COM(2011) 287 final.
30. <<http://europa.eu/rapid/pressreleasesaction.do?reference=ip/11/630&format=html&aged=0&language=en&guilanguage=en>>.
31. COM (2010) 245.
32. COM (2010) 2020.
33. COM (2011) 11.
34. COM (2011) 206.
35. COM (2010) 546.
36. For example the infamous French HADOPI law, which stipulates a graduated punishment mechanism for alleged copyright infringements on the Internet (Law No. 2009-1311 of 28 Oct. 2009 relating to the criminal protection of copyright on the Internet (Official Journal, 29 Oct. 2009)), the UK Digital Economy Act 2010 (<http://www.legislation.gov.uk/ukpga/2010/24/contents>), the Dutch Notice and Take Down Code of Conduct (In October 2008, the Netherlands designed a 'Notice-and-Take-Down Code of Conduct'. This Code provides for ISP liability especially in cases of hosting services where illegal content is involved and this is brought to the ISP's attention) and so on (Sweden (On 1 Apr. 2009, a new law was adopted in Sweden, which is based on the EU Enforcement Directive. This law allows copyright holders to obtain a court order forcing ISPs to provide the IP addresses identifying which computers have been

the European Union waits to regulate in this field, the harder will be for it to find a solution that will be acceptable to all Member States given the fact that some of them have already proceeded with their own solutions.

---

sharing copyrighted material. See <<http://news.bbc.co.uk/2/hi/technology/7978853.stm>>, Germany (German legislation which was passed in the German Parliament on 18 Jun. 2009. This legislation obliges ISPs to filter websites allegedly containing child abuse material. The secret filtering list shall be put together by the German Federal Police and transmitted to ISPs once a day with only occasional checks by a five-member monitoring body), Italy (On 26 January 2010, the Italian Government proposed legislation on the basis of which ISPs shall be responsible for their audiovisual content and liable for copyright infringement by users), Spain (On 8 January 2010, the Spanish Government passed the Law for Sustainable Economy. This Law provides, amongst other issues, for the creation of an Intellectual Property Commission (IPC) which, together with a judge, will deal with complaints concerning alleged illegal downloading. This law will give the authorities the possibility to shut down file-sharing sites within a few days from the date the complaint is filed with IPC. Within four days from such date, the court is to decide whether a certain site is infringing the law or not. See <[www.edri.org/edri-gram/number8.1/spain-law-file-sharing](http://www.edri.org/edri-gram/number8.1/spain-law-file-sharing)>. For more information see the relevant section on the Hellenic Copyright Organisation site <[www.opi.gr](http://www.opi.gr)> and I. Stamatoudi (ed), Copyright Enforcement and the Internet, Information Law Series (B. Hugenholtz (general editor), Kluwer Law International, 2010.

# **Evaluating the quality of e-democracy processes: an empirical study in the Greek context**

---

**Stiakakis Emmanouil &  
Tongaridou Konstantina**

---

## **1. Introduction**

Plato's philosophy about democracy in ancient Athens is considered to be the foundation of democracy upon which advanced post-monarchial regimes were established. Democracy of Athens can be used as a model for societal decision making in which all citizens are able to input their views and have an impact on government's policies. The ideal is the belief that freedom and equality are sacred and participation of citizens in governance enhances human dignity [Lan, 2005].

In the early 1990s, the emergence of a new medium, the Internet, offered the potential to connect citizens to decision-makers and raised high expectations of the advent of a more "Athens-style" democracy, as its democratic possibilities, such as information richness, decentralization, absence of censorship, and the rise of user-generated interactive platforms were glorified. The Internet now offers the equivalent of the open space in which free people gathered in ancient Athens to debate and decide on public affairs. However, there has been a shift from Plato's ideal to the new political means of communication, which encourage interaction between citizens and public officials providing a rich forum for discussion of contentious political issues [Milakovich, 2010]. Consequently, ICTs provide public authorities and government with tools to improve interaction and communication with citizens, design new ways to access and participate in democratic processes, and share the responsibility of political decision processes, leading to a new model of governance, the model of e-democracy.

The emergence of the model of e-democracy is beneficiary for all the stakeholders. Firstly, for the citizens, as they can express and share their views enhancing the bottom-up interaction, making communication more horizontal, and having a first-person voice in the political agenda. Secondly, for the political parties, as e-democracy contributes to the decrease of the democratic deficit, increasing the participation of mainly young people to the political processes. Thirdly, for the governments, as they enforce the transparency and the accountability on public issues with the application of the model of open government with open data and open communication channels [Peña-López, 2010].

However, the implementation of e-democracy is not without obstacles [Council of Europe, 2008]. There are mainly institutional barriers, as there may be such an increase in demand for e-democracy, such as e-participation, e-voting, etc., that the administrations can not cope with it. Additionally, it expands the digital divide between those who are connected to the Internet and those who are not, as well as between those who can exploit the Internet to a large extent and those who cannot. There are also legal barriers, as e-democracy requires rules and regulations that need to focus upon the needs of the citizen, while being carefully balanced. E-democracy should protect the citizens' rights, their privacy and personal data, as well as their intellectual property. However, regardless the barriers, e-democracy is above all about democracy and not simply about technology. Its main objective is to support democracy, democratic institutions, and democratic processes, as well as to contribute to the diffusion of democratic values [Council of Europe, 2009].

Undoubtedly, e-democracy is an uprising subject that many researchers have approached it, focusing mainly on the analysis of e-democracy sectors, such as e-participation [Cartwright and Atkinson, 2009; Macintosh, 2008, Peristeras et al., 2009], e-consultation [Nijland et al., 2009], e-voting [Spycher and Haenni, 2010; Backes et al., 2008].

In this paper, efforts have been made to shed light on e-democracy and more specifically the quality characteristics of e-democracy. The next section gives an overview of the definitions of e-democracy. Section 3 presents the various sectors of e-democracy, whereas Section 4 focuses on the models of e-democracy. Section 5 presents the "C2ST" framework, which is adopted in this study for the evaluation of the quality of e-democracy. The methodology of the study is included in Section 6, while a synopsis of our research findings is given in Section 7. Finally, this paper concludes in Section 8.

## 2. Definitions of e-democracy

There have been various definitions of e-democracy, depending on the perspective it can be seen. Earlier definitions mainly focus on the technological part and the so-called collaborative platforms, with the latest emphasizing mostly on the principles and values that are connected to. E-democracy can broadly be described as the use of ICTs to increase and enhance citizens' engagement in democratic processes [Milakovich, 2010; Shirazi et al., 2010; Yigit and Colak, 2010]. According to the Council of Europe, e-democracy could be described as the use of ICTs by "democratic sectors" within the political processes of local communities, regions, states, and nations [Council of Europe, 2009]. By the term "democratic sectors" the following items are meant [Clift, 2004]:

- Governments.
- Elected officials.
- Media (including online portals).
- Political parties and interested groups.
- Civil society organizations.
- International governmental organizations.
- Citizens – voters.

Through the use of different forms of ICTs, such as the Internet and mobile devices, there is the opportunity not only to carry out more effective work and organize it better but also to contact those who do not normally participate in political issues. In a bottom-up perspective, citizens and organisations can use the ICTs as resources to get their voice heard; political parties use them for campaigning, while public agencies for improving the quality of the services that they deliver to citizens.

In 2004, in the conference of the legislative federal state parliaments of Europe [Lizarralde et al., 2007] the following features of e-democracy were specified: “new technologies and communication in practice are extraordinarily useful for the public administrations in promoting the transparency of their activities, stimulating the public’s interest in what happens in the Parliament and offering the mechanisms to follow the decision making processes and participate in them. By using technologies in that way, we believe that they will contribute to the improvement of our democracy’s quality and add value to the role that our institutions are currently carrying out and, in short, foster efficiency and effectiveness in public policy”.

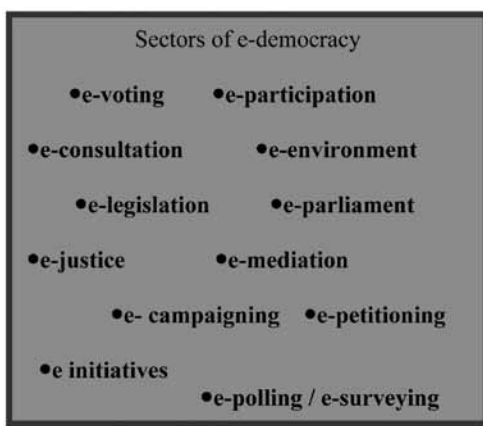
In 2006, ePlanIT, i.e., the Local e-Democracy National Project in Great Britain gave the following definition [Lizarralde et al., 2007]: “e-democracy is the use of ICTs, including the Internet, mobile technologies, and interactive digital television, to create new deliberative discussions between government and its citizens and between citizens themselves. It complements traditional methods of community engagement, such as public meetings and workshops so therefore it should not be viewed as a different model of democratic governance”.

Many researchers claim that there is no such a thing as electronic democracy, as exactly there is no such a thing as paper democracy; democracy is simply democracy, meaning that what the new digital technologies have changed is the environment in which democracy takes place. It makes no difference whether the citizens vote by hand or through digital means. On the contrary, Li [2010] claims that what characterizes e-democracy is the prefix for “electronic”. Being electron-

ic is not only a trivial but a fundamental and crucial difference from democracy in its classical meaning.

### 3. Sectors of e-democracy

According to the Recommendation of the Committee of Ministers to EU member states concerning e-democracy [Council of Europe, 2009], e-democracy includes e-parliament, e-legislation, e-justice, e-mediation, e-environment, e-voting, e-consultation, e-participation, e-initiatives, e-petitioning, e-campaigning, and e-polling / e-surveying (Figure 1). Based on the recommendation mentioned above, each one of the sectors is analyzed below:



**Figure 1.** Sectors of e-democracy

E-parliament is considered to be the use of ICTs by elected representative assemblies, their members, and political and administrative staff in the conduct of their tasks, in particular for the purposes of actively involving citizens. E-parliament concerns legislative, consultative, and deliberative assemblies at international, national, regional, and local level.

E-legislation is the use of ICTs for commenting on, consulting, structuring, formatting, submitting, amending, voting on, and publishing laws passed by elected assemblies. It makes legislative procedures more transparent, improves the content and readability of legislation, provides better access to it, and thereby enhances public knowledge of the law.

E-justice is the use of ICTs in the conduct of justice by all stakeholders of the judiciary in order to improve the efficiency and quality of the public services, in particular for individuals and businesses. It includes electronic communication and data exchange, as well as access to judicial information.



E-mediation is the use of ICTs to find the means of resolving disputes without the physical presence of the opposing parties; a lot of digital tools can serve as mediators.

E-environment is the use and promotion of ICTs for the purposes of environmental assessment and protection, spatial planning, and the sustainable use of natural resources. Using ICTs to introduce or enhance public participation can improve democratic governance in respect of environmental issues.

E-voting is an election or referendum that involves the use of electronic means in, at least, the casting of the vote. E-voting speeds up procedures, enables voting to be electronically monitored, and facilitates participation from greater distances and by persons with special needs.

E-consultation is a way of collecting the opinions of designated persons or the public at large on a specific policy issue without necessarily obliging the decision maker to act in accordance with the outcome. There are various forms of e-consultation, formal and informal, public-authority-regulated and unregulated.

E-participation refers to the active participation of citizens to political issues and policies. The democratic political participation must involve the mechanisms and means for allowing citizens to take part in the public decision-making process.

E-initiatives allow citizens to develop and put forward political proposals by means of ICTs, engaging them in political agenda setting.

E-petitioning is the electronic delivery of a protest or recommendation to a democratic institution. Citizens sign a petition and possibly engage in a discussion on the subject by putting their names and addresses online.

E-campaigning is carried out by electronic means, encouraging people to engage with one another in order to mobilise individuals in electoral and other campaigns and/or persuade them to promote a particular cause, in an endeavour directly or indirectly to influence the shaping or implementation of public policy.

E-polling/e-surveying allow opinions to be obtained informally, by electronic means, from random or selected persons, usually in connection with specific proposals and a set of possible responses.

#### **4. Models of e-democracy**

The models of e-democracy are frameworks that relate the use of technology to the various forms of political organizations, mainly emphasizing on the impact of ICTs on processes of public decision-making. According to our literature review, the following models are noteworthy to be mentioned:

- The four e-democracy models [Päivärinta and Sæbø, 2006] are based on two fundamental characteristics, namely, inclusion in decisions and control of

the agenda. Inclusion means that all adults who belong to a society should be allowed to participate in political debates and be involved in decision-making processes. Control of the agenda deals with the issue of who decides and what the decision should be about. In particular, this gives the right to the citizens to raise issues and actively participate in decision-making processes. The four e-democracy models are presented in Table 1.

Citizens set the agenda	Partisan e-democracy	Direct e-democracy
	Citizens express bottom-up opinions and criticize existing power structures. No explicit connection to the existing government or political decision-making processes is defined beforehand. Citizens set the agenda for public discussions, but not for decision-making. ICTs seek to obtain visibility for alternative political expressions uninterrupted by political elite.	Citizens participate directly in decision-making processes. The citizens are online affecting the decisions to be made (mostly at the local level). Citizens set the agenda for both public discussion and decision-making. ICTs are a crucial pre-condition for democracy to support coordination among decision-makers.
Government (politicians and officers) set(s) the agenda	Liberal e-democracy	Deliberative e-democracy
	Government serves citizens who participate in elections and related debates. Government would like to inform and be informed by the citizens. There is no clear connection to decision-making activities. ICTs seek to improve the amount and quality of information exchange between government and citizens.	E-democracy projects are used for specific purposes, involving citizens in public decision-making processes. Citizens have a good reason to expect that their voices are heard concerning a particular matter. ICTs are developed for increased citizen participation and involvement in decision-making processes.

**Table 1.** Models of e-democracy (Source: Päivärinta and Sæbø, 2006)


- The Organization for Economic Co-operation and Development [OECD, 2003] defines the following three types of e-democracy:

**Information:** a one-way relation in which the government produces and delivers information to be used by citizens. It covers both “passive” access to information upon demand by citizens and “active” measures by government to disseminate information to citizens (e.g. access to public records, governmental Web sites).

**Consultation:** a two-way relationship where citizens provide feedback on government’s issues as citizens take part in consultations initiated by the local authorities or the government with the aim of enhancing the community involvement in democratic processes (e.g. public opinion surveys, comments on draft legislation).

Active participation: a partnership relationship with government, where citizens are actively involved in the decision- and policy-making process. It is acknowledged the role of citizens in proposing policy options and shaping the policy dialogue, even though the final decision rests on the government.

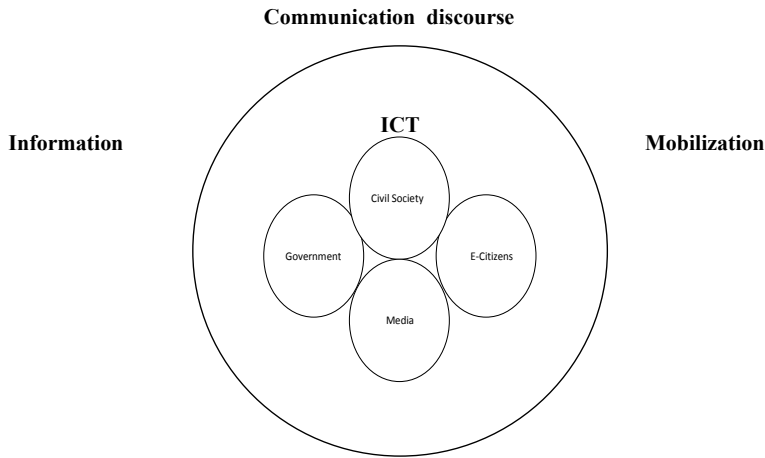
- The Institute of Electronic Development proposes a four-stage model of e-democracy, which is not limited to the citizen-to-government point of view, mapping the four progressive scenarios from an informed to an engaged citizen. It also serves as a scorecard of digital understanding of how successfully a governmental entity (an elected representative, a legislative body, a political party, etc.) interprets and responds to the digital world and exploits the technology accordingly to advance influence [Caldow, 2004]. This model helps leaders to implement tactical and strategic e-democracy efforts into an overall e-government strategy. At this point, it should be clarified that the tactical side of e-democracy refers to the fact that Information Technology has advanced communication and the access to information better than any known medium, while the strategic side tries to give an answer to the question “*how can a government use digital media to both actively engage citizens and advance its public policies to the world community?*” [Caldow, 2004]. Taking a look at this model, a government can identify its current position against characteristics at various sophistication levels and see what e-initiatives are needed to proceed to the next level. There are two axes, as shown in Table 2: the vertical axis measures the degree of engagement and the horizontal axis measures influence.

<p style="text-align: center;"><b>Quadrant Two</b></p> <p>E-mail Online opinion polls Online surveys Email alerts Electronic voting methods</p>	<p style="text-align: center;"><b>Quadrant Four</b></p> <p>E-petition E-consultation Policy Diplomacy Transparency Digital Divide</p> <p style="text-align: right;">GLOBAL DOMESTIC</p> 
<p style="text-align: center;"><b>Quadrant One</b></p> <p>Passive, One Way, Asynchronous Search information View Web casts Track legislation Look-up representatives</p>	<p style="text-align: center;"><b>Quadrant Three</b></p> <p>Collaborative, Interactive Dynamic monitoring of news media &amp; Internet Volunteer recruitment &amp; coordination Fundraising Online forum</p>

**Table 2.** A four-stage model of e-democracy (Source: Caldow, 2004)

Let us shortly analyze the four quadrants [Caldow, 2004]:

- Quadrant One: a fundamental step in e-democracy tactics for most governmental entities, such as governments, legislative bodies, international organizations, political parties, etc., is to make information available online. This can be measured, for example, by the frequency of the visits of Web sites in general, the visits of governmental Web sites by the citizens in order to search information for public policy issues (e.g., information about how to cast their votes).
- Quadrant Two: entities in this quadrant have made great efforts to start two-way communication. Every public institution and those who serve them are obliged to move beyond information dissemination to open two-way communication channels. The two-way communication includes the holding of online surveys and online polls, the use of e-voting methods, and the sending of e-mail messages to the governmental bodies and the politicians. Without any doubt, the entities that belong to this quadrant have achieved two-way capability, though its nature is still asynchronous, meaning that a percentage of the governmental bodies do not respond, for example, to citizens' demands.
- Quadrant Three: though still asynchronous, this quadrant extends interactive capability, meaning that communication begins to evolve into collaboration. Most visible in this stage are political players and the electoral process with tactics, such as recruiting and organizing volunteers online, online fundraising, campaigning, communication with constituents and the media, voter registration, and voting.
- Quadrant Four: it represents the highest level of e-democracy sophistication – strategic, interactive, synchronous, and global in nature.
- Clift's conceptual model, depicted in Figure 2, is composed of five components: ICT, e-citizens, government, civil society, and media [Shirazi et al., 2010].



**Figure 2.** Clift's conceptual model (Source: Shirazi et al., 2010)

*E-citizens* are individuals that use ICTs to participate in democratization process: citizens through the Internet can interact with social groups, political parties, the government, and they succeed in that way the creation and the dissemination of information, increasing their participation in the debates and the social dialogue.

*Civil society* includes national governmental organizations, trade unions, political organizations that use ICTs with the aim of "good" governance and democratic development.

*Government* in this model represents e-government that provides citizens, civil society, private sector, and media with excessive access to information electronically in order to support the functions that a government performs.

*Media* as ICTs have got the power to destabilize the control of the production and circulation of information held by the traditional media [Shirazi et al, 2010].

ICTs possess an interactive comparative advantage compared to the traditional mass media as regards the establishment of communication between citizen and politics, providing the political communication with new means and enhancing at the same time the direct democracy.

- The European e-Democracy working group for IT4ALL, comprising eight European regional parliaments with experience in e-Democracy projects, has defined and analyzed the key factors to support and enable e-democracy as below [Lizarralde et al., 2007]:
- Commitment: it refers, not only to the achievement of objectives, but also to the formation of the basis on which the strategic design and the corporate

culture of the representative institutions are supported. This includes the budgetary undertakings and the measures that the organizations should take and are linked to the specific values.

- **Transparency:** the public institutions are obliged to operate with openness and facilitate participation of citizens in their decision-making processes.
- **Proactivity:** the information and participation mechanisms that enable the new technologies should simplify the process of obtaining information and establish proactive services, while at the same time the organizations should provide original and complete information in real-time, arranged with the demand defined by the citizens and their organizations.
- **Multi-channel:** ICTs are useful tools for the application of the principles of transparency, participation, openness in the decision-making process, though the possibilities offered by ICTs should be combined with those offered by the traditional means of communication (e.g., telephone, radio, television).
- **Training in civic values:** the public institutions should encourage the citizen participation in the decision-making processes by simplifying languages and procedures, giving maximum visibility to the results arising from civic contributions. Additionally, training should be provided to the youngest in society concerning issues of responsibility and participation.

Based on the above key factors, the e-democracy model with the key factors has been formed and can be viewed as an incremental process that is comprised by the following stages:

- On an initial stage, services of openness and transparency are stressed as unidirectional services from public authorities to citizens.
- On a second stage, pro-active services appear, promoting bi-directional flow of information, such as services to submit queries, suggestions, etc.
- On the last stage, the services that appear promote dialogue and discussion among citizens, including deliberations on information needed as a basis for decision-making and suggestions to improve and encourage active citizen participation, as citizens are able to decide by voting, consultation or a well structured referendum [Lizarralde et al., 2007].

## **5. The quality framework to evaluate e-democracy**

The quality framework to evaluate e-democracy is structured on the basis of a business process, i.e., the collection of related and structured activities undertaken by one or more organizations in order to pursue some particular goals [Cor-

radini et al., 2009]. The execution of a business process involves humans, software applications, documents, methods, and techniques to design, control, and analyze operational activities, while there is sometimes interrelation among the business processes within the same or other organizations [Lindsay et al., 2003]. The business process plays a crucial role in the success of a business activity and for that reason in the recent years the Business Process Management (BPM) has been developed to denote that the entire management of an organization – strategy, goal setting, controlling and planning – should be based on its core processes. Quality plays a crucial role for the BPM and it is remarkable that quality models have reinforced the implementation of BPM, such as Total Quality Management [Bandara et al., 2007].

The business process of the quality evaluation of e-democracy refers to all the activities and methods that should be taken in order to implement the e-democracy project, involving all the stakeholders, i.e., citizens, government, civil society, and media. In our paper, we have tried to identify specific quality requirements for e-democracy combining the “C2ST”, i.e., a four dimensional quality framework for the delivery of e-services [Corradini et al., 2009] with the models of e-democracy.

The C2ST dimensional framework refers to the assessment of e-services delivery according to the four quality dimensions, while it should be clarified that the implementation of each quality dimension requires different business process levels. The C2ST framework considers the following dimensions [Corradini et al., 2009]:

**Co-ordination:** the term co-ordination means the capability of two or more public administrations to work together with the aim of accomplishing common goals using ICTs through the delivery of a governmental digital service to a citizen. It is clear that in the e-government coordination, people and information systems play a significant role for the implementation of a specific service.

**Control:** the quality dimension of control includes the proactive control in the provision of the e-service; the administration may work as a proactive participant as the e-service may be available through direct communications to interested citizens providing precise references. Generally, it refers to the policies that should be activated with the aim of achieving the service delivery from its start to its final fulfillment.

**Sharing:** it refers to the way in which the public authorities handle and share citizens' data with other administrations in order to participate in the delivery of a specific service, as it is widely acceptable that citizens generally feel uncomfortable when they use a service that asks for authorization to store citizens' data.

Transparency: it is the ability of the administrations to make citizens aware of the delivery process so as to improve citizens' trust and inclusion, as citizens feel more satisfied when they have got a clear and reliable view on how the service is delivered.

Based on the above C2ST four-dimensional quality framework for the delivery of e-services, we have attempted to structure the quality framework for the evaluation of e-democracy, i.e., the C2ST framework adjusted to the e-democracy context. The suggested quality framework for e-democracy consists of four quality dimensions, as described below:

### ***Co-ordination***

In the quality evaluation of e-democracy, co-ordination refers to the degree of co-operation between public authorities using ICTs. This degree of co-operation dramatically affects the implementation of e-democracy. The harmonious cooperation of all the stakeholders involved in the implementation of e-democracy is a prerequisite for the function of e-democracy in the different stages and the different sectors (e-participation, e-consultation, etc.) that it is implemented.

### ***Control***

This dimension refers to the specific, original, complete information given for e-democracy by the authorities for the implementation of e-democracy with the aim of increasing the control of the politicians. Governments should play a proactive role in the online world. Firstly, it is necessary to maintain existing democratic practices in spite of pressures coming from the information age. Secondly, they should adapt and incorporate online strategies and technologies with the aim of leading efforts that expand and enhance democracy.

### ***Sharing***

In the e-democracy framework, sharing refers to the way in which the public authorities handle and share citizens' data with other administrations. The protection of personal data is a key principle for e-democracy since the citizens need to be aware that their personal data are used only for the purpose they are given. E-democracy processes should protect above all citizens' rights, their privacy and personal data, as well as their intellectual property. Public authorities should take all the necessary legal measures in that direction. Otherwise, citizens' trust on e-democracy may be lost and as a consequence, the whole project of e-democracy will be jeopardised.



### ***Transparency***

In e-democracy, the dimension of transparency refers to the obligation of the institutions to operate with openness and to make citizens fully aware of the decision making-process, aiming at facilitating their participation. Transparency improves citizen's trust on the political system as it constitutes a layman's basic map of the organization as depicted in the information on the site and reveals the depth of access it allows, the depth of knowledge about processes it is willing to reveal, and the level of attention to the citizen [Weich and Hinnant, 2003].

## **6. Methodology**

We applied confirmatory factor analysis to investigate whether the four aforementioned dimensions of e-democracy are indeed the core dimensions of this construct. The dimensions of e-democracy were analyzed to specific quality criteria as follows (the corresponding variables are given in parentheses):

### *Coordination:*

- E-democracy presupposes the design and development of an integrated information system in every public agency (v37).
- Integrating the information systems of all public agencies is a necessary condition for the fulfilment of e-democracy (v38).
- The personnel of a public agency responds much better when the citizens' requests concerning issues of authority exercise are electronically submitted (v39).
- The coordination of the acts of the personnel of all public agencies is a necessary condition for the fulfilment of e-democracy (v40).

### *Control:*

- E-democracy reinforces the control of central government by citizens (v41).
- Citizens are able, through the Internet, to express their opinions and control the activities of politicians (v42).
- E-polling results constitute a tool of developing and controlling the governmental policies (v43).
- E-consultation, e-legislation, and e-petitioning assist citizens to control the Parliament's functioning (v44).

*Sharing:*

- The personal data of citizens are protected in an e-democracy system (v45).
- Citizen's data transfer from one public agency to another public agency explicitly assumes citizen's authorization (v46).
- The accomplishment of political campaigns through the Internet contributes to sensitization and mobilization of citizens regarding political issues (v47).
- Citizen's awareness regarding e-legislation makes easier the implementation of the law (v48).

*Transparency:*

- E-voting results are reliable and valid (v49).
- Citizens get fully informed, through the Internet, about governmental authority issues (v50).
- E-democracy enhances citizen's trust to the democratic rules (v51).
- E-participation makes the political decisions more transparent (v52).

The sixteen quality criteria, formulated in the way mentioned above, were rated by means of a survey conducted among citizens in the broader area of Thessaloniki, Greece. Since the survey is still in progress, the sample size used in this work was 208 citizens without any constraints concerning the gender and their occupation. The only constraints pertained their age (over than 18 years old) and education (at least secondary education graduates). The sample size was acceptable for factor analysis, since the minimum size required is five times the number of variables, i.e., 80 individuals. The data were collected through personal interviews and electronic mail messages using a structured questionnaire, which is divided into three main sections (familiarization with e-democracy sectors, assessment of benefits and obstacles of e-democracy, and, rating of e-democracy quality criteria). For the purpose of rating the quality criteria, a five-point Likert scale was used (i.e., strongly agree, agree, neither agree nor disagree, disagree, strongly disagree).

We selected Principal Component Analysis (PCA) as a factor extraction method. It should be mentioned that when the values of most of the communalities (estimates of variables' common variance) exceed the value 0.6 (as indicated in Table 8), then PCA and common factor analysis provide essentially identical results.

## **7. Research findings**

Table 3 shows the communalities of the variables v37 to v52, which correspond to the quality criteria in which the four dimensions of e-democracy, namely, co-

ordination, control, sharing, and transarency, were analyzed. As indicated in the table, all the communalities get high values, meaning that all the variables relate to certain components.

Variable	Initial	Extraction
v37	1.000	0.689
v38	1.000	0.618
v39	1.000	0.432
v40	1.000	0.67
v41	1.000	0.69
v42	1.000	0.604
v43	1.000	0.515
v44	1.000	0.702
v45	1.000	0.365
v46	1.000	0.697
v47	1.000	0.413
v48	1.000	0.396
v49	1.000	0.626
v50	1.000	0.684
v51	1.000	0.674
v52	1.000	0.603

**Table 3.** Communalities (extraction method: Principal Component Analysis)

The eigenvalues, i.e. the percentages of each variable's variance which is accounted for by the component, are presented in Table 4. The table shows 16 components, as exactly the number of the variables. However, the eigenvalues are high (over than the unity) only for 4 components. As we can see in the last column, 58% of the total variance is accounted for by four components (in general, a percentage over than fifty per cent is considered satisfactory).

Component	Eigenvalue	% of Variance	Cumulative %
1	5.209	32.556	32.556
2	1.725	10.784	43.34
3	1.229	7.683	51.023
4	1.154	7.211	58.235
5	.901	5.632	63.866

6	.876	5.478	69.344
7	.76	4.747	74.092
8	.629	3.934	78.026
9	.615	3.843	81.869
10	.572	3.577	85.446
11	.499	3.12	88.566
12	.461	2.878	91.445
13	.45	2.811	94.256
14	.375	2.346	96.601
15	.293	1.832	98.433
16	.251	1.567	100

**Table 4.** Total variance explained

The Rotated Component Matrix, in Table 5, shows the loadings, i.e. the correlations between the variables and the corresponding component. Rotation converged in 5 iterations. The first component has high loadings for the variables v37 to v40, the second one for the variables v41 to v44, the third one for the variables v45 to v48, and finally the fourth component has high loadings for the variables v49 to v52. It is reminded that the variables v37-v52 correspond to the sixteen quality criteria, which comprise the four core dimensions of e-democracy.

Variable	Component			
	1	2	3	4
<b>v37</b>	<b>0.784</b>	0.208	0.136	-0.227
<b>v38</b>	<b>0.773</b>	0.023	0.088	-0.173
<b>v39</b>	<b>0.723</b>	-0.03	-0.041	0.274
<b>v40</b>	<b>0.586</b>	0.214	0.289	0.159
<b>v41</b>	0.07	<b>0.571</b>	0.202	0.157
<b>v42</b>	-0.005	<b>0.806</b>	0.313	-0.191
<b>v43</b>	-0.042	<b>0.75</b>	0.19	0.046
<b>v44</b>	0.274	<b>0.559</b>	0.009	0.05
<b>v45</b>	0.092	0.233	<b>0.818</b>	-0.045
<b>v46</b>	0.133	-0.087	<b>0.736</b>	0.269
<b>v47</b>	0.13	0.189	<b>0.494</b>	0.114
<b>v48</b>	0.141	-0.24	<b>0.43</b>	0.282

<b>v49</b>	0.173	-0.211	0.301	<b>0.653</b>
<b>v50</b>	-0.083	0.064	-0.172	<b>0.537</b>
<b>v51</b>	0.049	0.117	0.038	<b>0.768</b>
<b>v52</b>	-0.262	0.192	0.065	<b>0.471</b>

Extraction Method: Principal Component Analysis  
Rotation Method: Varimax with Kaiser Normalization  
Table 5. Rotated component matrix

## 8. Conclusion

According to the findings of confirmatory PCA, the sixteen quality criteria were properly grouped into the four core dimensions of e-democracy, i.e., coordination, control, sharing, and transparency. This work should be considered as a step to better comprehend the construct of e-democracy. This can only be done through the analysis and further examination of its components. In order to validate even more the quality framework of the four core dimensions, it is suggested to test it in other countries, where citizens are more familiar with the concept of e-democracy. This is a limitation of our study since the majority of Greeks have not seen in real life many of the aspects of e-democracy. Moreover, the assessment of the relative importance of the four dimensions is a topic which needs further consideration.

## References

- Backes M., Hritcu C. and Maffei M. (2008), Automated verification of remote electronic voting protocols in the applied Pi-Calculus, *Proceedings of the 21<sup>st</sup> IEEE Computer Security Foundations Symposium*, IEEE Computer Society, Washington DC, USA, 195-209.
- Bandara W., Indulska M., Chong S. and Sadiq S. (2007), Major issues in Business Process Management: An expert perspective, *Proceedings of the 15<sup>th</sup> European Conference on Information Systems*, St. Gallen, Switzerland, 1240-1251.
- Caldow J. (2004), e-Democracy: Putting down global roots, online at <http://www-01.ibm.com/industries/government/ieg/pdf/e-democracy%20putting%20down%20roots.pdf> / accessed 20.02.2011.
- Cartwright D. and Atkinson K. (2009), Using computational argumentation to support e-participation, *IEEE Intelligent Systems*, 24(5), 42-52.

Clift S.L. (2004), e-Government and democracy – Representation and citizen engagement in the information age, online at <http://www.publicus.net/articles/cliftegovdemocracy.pdf> / accessed 11.03.2011.

Corradini F., Hinkelmann K., Polini A., Polzonetti A. and Re B. (2009), C2ST: A quality framework to evaluate e-government service delivery, *Proceedings of the 8<sup>th</sup> International Conference EGOV*, Linz, Austria, 74-84.

Council of Europe (2008), e-Democracy: Who dares?, Forum for the future of Democracy 2008 Session, Madrid, Spain.

Council of Europe (2009), Directorate General of Democracy and Political Affairs, Directorate of Democratic Institutions, Project: “Good governance in the information society”, Indicative Guide No. 5 Recommendation of Committee of Ministers to member states on e-democracy.

Lan L. (2005), Enhancing e-democracy via fiscal transparency: A discussion based on China’s experience, *EGovernment Towards Electronic Democracy*, 3416, 57-69.

Li B. (2010), To “e-” or not to “e-” – Re-locating innovation in “electronic” decision-making, *Journal of eDemocracy*, 2(2), 145-161.

Lindsay A., Downs D. and Lunn K. (2003), Business processes – attempts to find a definition, *Information and Software Technology*, 45(15), 1015-1019.

Lizarralde O., Goikolea J., Sagardui G. and Goikoetxea A. (2007), E-democracy factors and IT-governance factors for a best implementation of e-democracy projects and strategies in public authorities, *IADIS International Journal on WWW/Internet*, 5(2), 58-71.

Macintosh A. (2008), e-Democracy and e-participation research in Europe, in *Digital Government: E-Government Research, Case Studies, and Implementation*, Vol. 17, Unit I, 85-102.

Milakovich M. (2010), The Internet and increased citizen participation in government, *Journal of eDemocracy & Open Government*, 2(1), 1-9.

Nijland N., van Gemert-Pijnen J.E., Boer H., Steehouder M.F. and Seydel E.R. (2009), Increasing the use of e-consultation in primary care: Results of an online survey among non-users of e-consultation, *International Journal of Medical Informatics*, 78(10), 688-703.

OECD (2003), Promise and problems of e-democracy: Challenges of online citizen engagement, online at <http://www.oecd.org/dataoecd/9/11/35176328.pdf> / accessed 19.02.2011.

Päivärinta T. and Sæbø O. (2006), Defining the “e” in e-democracy: A genre lens on IT artefacts, online at <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.94.3334> / accessed 08.03.2011.

Peña-López I. (2010), Goverati: e-Aristocrats or the delusion of e-democracy, online at [http://ictlogy.net/articles/20100506\\_ismael\\_pena-lopez\\_-\\_goverati\\_e-aristocrats\\_delusion\\_e-democracy.pdf](http://ictlogy.net/articles/20100506_ismael_pena-lopez_-_goverati_e-aristocrats_delusion_e-democracy.pdf) / accessed 07.03.2011 / accessed 13.03.2011.

Peristeras V., Mentzas G., Tarabanis K.A. and Abecker A. (2009), Transforming e-government and e-participation through IT, *IEEE Intelligent Systems*, 24(5), 14-19.

Shirazi F., Ngwenyama O. and Morawczynski O. (2010), ICT expansion and the digital divide in democratic freedoms: An analysis of the impact of ICT expansion, education and ICT filtering on democracy, *Telematics and Informatics*, 27(1), 21-31.

Spycher O. and Haenni R. (2010), A novel protocol to allow revocation of votes in a hybrid voting system, *Proceedings of the 9<sup>th</sup> Annual Conference on Information Security*, Sandton, South Africa.

Welch E.W. and Hinnant C.C. (2003), Internet use, transparency, and interactivity effects on trust in government, *Proceedings of the 36<sup>th</sup> Hawaii International Conference on System Sciences*, IEEE Computer Society, Washington DC, USA, 1-7.

Yigit E.O. and Colak K. (2010), The opinions of the pre-service teachers about e-democracy in Turkey, *Procedia – Social and Behavioral Sciences*, 2(2), 712-716.

# The principle of technological neutrality in European copyright law: myth or reality?

---

Tatiana – Eleni Synodinou

---

The principle of technological neutrality has become famous but most of the time we cannot find an accurate definition of it<sup>1</sup>. In the field of telecommunications, it is often defined as the principle which states that all users should have an equal access to the network, independently of their usage or device<sup>2</sup>. Such principle is supported by the European Commission<sup>3</sup>. But also, more surprisingly, the principle has from time to time emerged in discussions about copyright law. What could be the meaning of this principle in the field of copyright law?

In a society that becomes more and more complex and dependent on technology, can the law remain technologically neutral? If we define technological neutrality of the law as the ability of legal mechanisms to comprehend technological evolutions independently of specific technologies, it is clear that technological neutrality is necessary for the survival of law over time.

Copyright law is strongly connected to technological evolutions. A dialectic relationship of copyright law to technology is generally accepted. Technology brings new challenges to copyright law, while copyright law tends to react initially by fighting and subsequently by encompassing the new ways of exploiting copyrighted works developed by the new technologies. Conversely, copyright law shapes technology by influencing the emergence of certain new technologies and

- 
1. For a distinction of the various transition stages of Internet neutrality, see N.A.N.M. van Eijk, About Network Neutrality 1.0, 2.0, 3.0 and 4.0, *Computers & Law Magazine*, 2011-6. See also: *Chris Marsden*, *Net Neutrality, Towards a Co-regulatory Solution*, Bloomsbury Academic, 2010 (download version: <http://ssrn.com/abstract=1533428>).
  2. In this context, the argument that peer-to-peer applications shall have lower access to broadband could be criticized.
  3. On 30 June 2010, the European Commission launched a public consultation on 'The open internet and net neutrality in Europe', in order to provide an evidence base for its forthcoming report to the European Parliament and Council on these issues. The consultation closed on 30 September 2010. The report on the public consultation on "The open Internet and net neutrality in Europe" of 9<sup>th</sup> of November 2010 provides an overview of the responses given from the stakeholders: [http://ec.europa.eu/information\\_society/policy/ecomm/doc/library/public\\_consult/net\\_neutrality/report.pdf](http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/report.pdf).



their design and architecture<sup>4</sup>. However, the organic link of copyright law with technology has not generally resulted to a tailor made legal construction which is shaped upon specific technological developments. From the invention of printing to the digital era, copyright law has been adapted in order to protect new categories of works and reflect new ways of reproduction and communication of works, but has kept a mainly technologically neutral character. Especially, in the information society technological neutrality should guarantee that for copyright owners and well as users, the concepts of copyright law apply equally regardless of the format of the work, whether analogue or digital<sup>5</sup>.

The language of copyright neutrality has quite a bit of appeal for copyright policy makers, since the fantasy of a law that adapts automatically to new innovation appeals to a legislative sense of economy<sup>6</sup>. At the same time, the dogma of the technological neutrality of copyright law has sometimes been denounced as an excuse for the excessive extension of its proprietary protection to the detriment of copyright exceptions and limitations in the digital environment<sup>7</sup>.

The first part of this article examines the independence of the core of European copyright law to technology as it is expressed through the fundamental concepts of this law and to underline the limits of this principle. Indeed, certain conditions for the award of protection which can be found mainly in the countries following the common law tradition, such as the requirement of fixation together with the adoption of a closed list of categories of protected works of mind, express a certain dependence of the work to its tangible form which seems to undermine the dogma of neutrality.

---

4. *Montagnani M.L.*, A new interface between copyright and technology: How user-generated content will shape the future of on-line distribution, <<http://ssrn.com/abstract=1275326>>· *Elkin-Koren N.*, Making technology visible: liability of Internet service Providers for peer to-peer traffic, 9 N.Y.U. Legis. & Pub. Pol'y 15-16 (2006).

5. *Litman T.*, The myth of technological neutrality in copyright and the rights of institutional users: Recent legal challenges to the information organization as mediator and the impact of the DMCA, WIPO, and TEACH, *Journal of the American Society for Information Science and Technology* 54, no. 9 (2003): 824-835.

6. *Smith K.*, technological neutrality as a rhetorical strategy, October 18th, 2009, <<http://blogs.library.duke.edu/scholcomm/2009/10/18/technological-neutrality-as-a-rhetorical-strategy/>>.

7. According to Litman, the ascendancy of digital ownership rights threatens to undermine the concept of technological neutrality, which in essence guarantees that ownership and well as "use" rights apply equally to analog and digital environments: *Litman T.*, The myth of technological neutrality in copyright and the rights of institutional users: Recent legal challenges to the information organization as mediator and the impact of the DMCA, WIPO, and TEACH, *op.cit.*

In the second part, it will be demonstrated that despite the theoretical dogma of technological neutrality, in certain cases the dependence of the work of mind to its medium renders copyright law less neutral as to the technology than it is generally declared.

## **1. The independence of copyright law to technological evolution**

The adaptation of copyright law to technological evolutions has been mainly expressed through the suppleness of its basic concepts, which has traditionally permitted the extension of copyright protection to new types of works of mind and to new techniques of reproduction and communication of works. The ability of copyright law to enclose new technologies is, nonetheless, limited by some particular rules and principles which partially undermine, but under no circumstances counteract a general tendency towards technological neutrality.

### ***1.1. The fundamental concepts of copyright law in the information society***

Technological neutrality of copyright law is mainly due to the vague character of its fundamental concepts as regards the existence, the content and the scope of copyright protection. Indeed, the research for neutrality is certainly a battle between vagueness and precision.

The central pillar of technological neutrality in copyright law is the concept of work. The concept of work is necessarily imprecise<sup>8</sup> and it is conceived in an open ended manner; these characteristics guarantee the ability of copyright law to comprehend the unimaginable ways of expression of human creativity. The technological neutrality of the concept of work permitted copyright law to protect new categories of works which derive from the application of new technologies, such as computer programs, video games, multimedia and electronic databases.

Legal doctrine and case law contributed to this evolution through the adoption of a lower standard of originality in the cases of works where the application of technologies seems *prima facie* to be more prominent than creative human intellectual activity. In this context, the concept of objective originality could be considered as a means of promoting technological neutrality in copyright law. Since objective originality is mainly sought in the qualities of the work itself regardless of the mark of personality of the author, it permits to extend copyright protection to the results of intellectual activity, which present a technical or industrious

---

8. Lucas A., *Traité de la propriété littéraire et artistique*, n°45, p. 53.

character, where the stamp of the author is not obvious or even absent<sup>9</sup>. The most illustrative example of the flexibility of copyright law to encompass technological achievements is the protection of software, which is undeniably a particular kind of literary work, given that it is not destined to communicate messages or feelings between humans but to make a machine to execute a specific task. The independence of copyright law towards technology brings copyright law closer to industrial property, which is traditionally perceived as a mechanism of promoting innovation.

The technological neutrality of copyright law is also expressed through the core of the main economic rights of the author, which apply broadly in the information society, the right of reproduction and the right of communication to the public.

The right of reproduction is defined in a very broad and all encompassing manner both in the international and European level. Article 9 par. 1 of the Berne Convention clearly states that the right covers reproductions of works in any manner or form. The Infosoc Directive recognizes the exclusive right to authorize or prohibit direct or indirect, temporary or permanent, reproduction by any means and in any form of the works and other protectable subject matter<sup>10</sup>.

Especially in the field of the right of reproduction, the pursuit of an effective protection of the author in the digital environment has led to the following paradox. The right of reproduction ended up to cover every use of the work in the digital environment, since the access of the work through a computer necessarily prerequisites a series of temporary reproductions of the work<sup>11</sup>. In this context, it could be argued that the prevailing technological neutrality of the right of reproduction is inconsistent with the aim of the award of the protection, which is not the control of every single act that gives access to the work, but the control of unauthorized acts of exploitation of the work<sup>12</sup>. Moreover, the all encompassing and technological neutral character of the right of reproduction blurred the con-

---

9. For the application of a criterion of objective originality in France as regards the protection of computer programs see the landmark Pachot case: CourCass, Ass. Plén., 7 mars 1986, JCP 1986, II, note *Mousseron, Teyssié et Vivant*.

10. Article 2 of the Infosoc Directive (Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society Official Journal L 167, 22/06/2001 P. 0010 – 0019).

11. This is the so-called “access right” which has been promoted by some scholars. See *Heide, T.*, Copyright in the E.U. and United States: what “access right”?, E.I.P.R. 2001. 469; *Ginsburg, J.*, From having copies to experiencing works: the development of an access right in U.S. copyright law, <[http://papers.ssrn.com/paper.taf?ABSTRACT\\_ID=222493](http://papers.ssrn.com/paper.taf?ABSTRACT_ID=222493)>.

12. As Professor Koumantos highlighted, “the uses of a work which are inter-connected as parts of an unified process and which either constitute necessary preparatory acts or natural con-

ceptual limits between the right of reproduction and communication to the public, since certain types of communication of a work, such as streaming<sup>13</sup>, imply both the creation of temporary transient copies and the application of the making available right<sup>14</sup>.

The side effect of this extension was the creation of a new mandatory exception, the temporary copy exception of article 5 (1) of the Infosoc Directive<sup>15</sup>, which paradoxically lacks of technological neutrality, since it is destined to apply only in a digital or in a network environment. This contradiction could have been avoided if the European legislator had chosen to define the right of reproduction in a way that excludes the creation of temporary copies of a pure technical character from the scope of protection<sup>16</sup>.

A specific demonstration of the will to promote the independence of copyright law regarding technology is the interoperability exception of the Software Direc-

---

sequences of the individual economic uses of the work shall not be considered as distinct ways of exploitation of the work": *Koumantos G.*, Copyright law, 2002, p. 203 (in Greek).

13. For an analysis of the economic rights involved in communication of works of mind through streaming see: *Borghi M.*, Chasing copyright infringement in the streaming landscape, IIC 3/2011, p. 316-343.
14. IVIR, Study on the Implementation and Effect in Member States' Laws of Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, report to the European Commission, DG Internal Market, February 2007, p. 25, <<http://www.ivir.nl>>. As it is stated in the Study: "...the distribution over the Internet now more often than not involves acts of reproduction as well as acts of communication (broadcasting or making available) and therefore requires double authorization. For instance, right holders have claimed remuneration for webcasting based on the argument that it not only constitutes communication to the public, but also reproduction because of the intermediate copies made during the streaming process". According to Professor A. Lucas, digital technology multiplies the cases of intersection of these rights. However, the distinction between the two rights still has sense and must be retained: *Lucas A.*, Litec, 1998, Droit d'auteur et numérique, p. 135, n° 266.
15. "Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable: (a) a transmission in a network between third parties by an intermediary, or (b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2".
16. For example, the Dutch legislator chose not to implement the broad definition of article 2 of the Directive and kept the existing national definition which excluded copies which present a technical character from the scope of the right. See: *Hugenholtz B.*, The Implementation of Directive 2001/29/EC in the Netherlands, RIDA, n°205, Octobre 2005, p. 121-122.

tive<sup>17</sup>. The aim of the exception is the possibility of communication of a computer program with other computer programs or with hardware. In other words, the exception enables software to apply and operate in all environments regardless of specific technological features and restrictions. Even though the effectiveness of this exception has been doubted, the establishment of the exception is an indirect, but a specific recognition of neutrality in the field of software protection, which aims to promote innovation and technological progress.

### ***1.2. The limits of the independence: the scope of copyright protection***

The dogma of technological neutrality as regard to the basic concepts of copyright law cannot be seriously doubted when considering the criteria for protection and the scope of economic rights of the author. Nevertheless, even in these fields neutrality is subject to certain limits.

Firstly, technological neutrality is restricted by the requirement of fixation. Indeed, some national legal systems following the common law tradition provide that copyright applies only to works which have been fixed in some material form<sup>18</sup>. In this context, oral works and other works which have not been fixed in a tangible medium, such as live music improvisations or choreographic works, do not receive copyright protection. In the field of new technologies, the lack of fixation of the work was discussed in the past in the case of video games, where it was debated whether there was not any stable and permanent display of the work due to the participation of the players which made the display of the game appear different every time<sup>19</sup>.

Secondly, the adoption of an exhaustive list system barring categories of works of mind<sup>20</sup> renders copyright less tolerant to new types of works which cannot fit di-

---

17. For an analysis of the exception see: *Beer-Gabel/ R. Chemain*, La décompilation des logiciels: l'industrie européenne face au droit d'auteur, *Revue trimestrielle du droit européen*, 27 (3) juillet-septembre 1991, p. 371. *Bitan H.*, Protection et contrefaçon des logiciels et des bases de données, *Directives européennes et transpositions, protections techniques et interopérabilité, expertise, jurisprudences française et anglo-saxonne*, *Axe Droit*, Lamy, 2006, p. 66. *Strowel A./Derclaye E.*, Droit d'auteur et numérique: logiciels, bases de données, multimédia, *Droit belge, européen et comparé*, Bruylant, Bruxelles 2001, p. 235.

18. Article 2 (2) of the Berne Convention leaves freedom to the Members of the Union on this issue.

19. *Midway Mfg Co. v. Artic International, Inc.* 794 F 2d, at 1011.

20. A closed list system is adopted in countries of the common law tradition, such as UK, Ireland and Cyprus. For an analysis of the principle in the UK copyright law see: *Bently L. and Sherman B.* (2009), *Intellectual property law*, 3<sup>rd</sup> edition, Oxford University Press, p. 58-59.

rectly within the existing categories<sup>21</sup>. An illustrative example is the case of multimedia products. If they cannot be classified in one of the existing categories, they cannot qualify for copyright protection. At the same time, forcing multimedia products to fit into one of the given categories of works-, for example in the category of computer programs or the category of dramatic works-, will result to the protection of the parts of the multimedia work which match with the characteristics of this category and, therefore, fail to protect the new work as a whole with all its additional features<sup>22</sup>.

Nevertheless, these findings shall not result to the denial of the principle of neutrality in both cases. A flexible interpretation of the term “fixation” could lead to the fulfillment of this requirement even in cases of non permanent digital fixations<sup>23</sup>. At the same time, the obstacle of a closed list of categories of works of mind is not insurmountable. Works of mind which do not directly fit into the established categories of works could be possibly awarded protection if the given categories are interpreted widely and in a technology neutral manner<sup>24</sup>.

A breach to the principle of technological neutrality as regards to the existence of copyright can be exceptionally found in the field of artistic copyright due to the impossibility to apply the idea/expression dichotomy in certain works of conceptual art. In fact, in particular cases there can be no clear distinction between the method or the technique which is applied to produce the work and the form of the work<sup>25</sup>. For example, the technique to create a work by compressing metallic automobile parts and shaping them in the form of cubes ends up to be indirectly protected through the protection of the specific work which has been created by the application of this technique. Consequently, irrespectively of the dogma of neutrality, copyright law finally protects rather a specific technique than a specific work.

---

21. See *Bandley B.* (2007), Over-categorization in copyright law: computer and internet programming perspectives, *E.I.P.R.* 29 (11), p. 461-465.

22. *Stamatoudi I.* (2002), Copyright and multimedia works, *A Comparative Analysis*, Cambridge Studies in Intellectual Property Rights, p. 192.

23. For a legislative example outside Europe, see the statutory requirement for copyright in US, which states copyright protection subsists in original works of authorship fixed in any tangible medium or expression, now known or later developed (17 U.S.C. §102(a)).

24. *Aplin T.* (2009), in: *E. Derclaye research handbook on the future of EU copyright*, Edward Elgar, p. 74.

25. For the difficulties of the application of the idea/expression dichotomy in the field of conceptual art, see: *Walravens N.* (2005), *L'œuvre d'art en droit d'auteur, Forme et originalité des œuvres d'art contemporaines*, Ed . ECONOMICA, p. 249.

Deviations to the principle of neutrality can also be found as regards the scope of protection and more specifically copyright exceptions and limitations. Particular importance shall be given to the private copy exception. While technological neutrality should have required that the exception applies without variations in the analog and in the digital environment, the Infosoc Directive does not fully guarantee the application of the exception in the digital environment, since it permits that the exception is overruled by the application of technological protection measures<sup>26</sup>. Moreover, the exception does not apply to electronic databases<sup>27</sup> and computer programs<sup>28</sup>. In this context, it is obvious that as regards the private copy exception the policy argument that “digital differs” has prevailed over the principle of technological neutrality.

## 2. The dependence of the work of mind to its medium

The question of the independence of copyright law as regard to technology takes a totally different dimension, if the point of reference is the relation of the work with its medium. As it will be demonstrated, despite the growing dematerialization in the information society, in certain cases the technological features of new media and of new ways of dissemination of works of mind seem to promote a strong technological dependence of work of mind to its medium in a way that technological neutrality could be described more as a chimera than a prevailing rule.

### 2.1. *Format shifting and economic rights*

A fundamental principle of copyright law is the complete independence of the work as an intangible resource to the tangible medium that incorporates the work<sup>29</sup>. Regarding the user rights, the application of this principle signifies that the owner of the tangible medium does not possess any right to the work itself, unless copyright prerogatives are transferred or licensed to her by the copyright

---

26. As regards the private copy exception Member states are not obliged to take legislative measures to help the beneficiaries of the limitation to benefit from it regardless of the application of technological measures. See: article 6 (4) of the Infosoc Directive.

27. Article 6 (2) (a) of the Database Directive states that Member states shall have the option of providing for limitations on the rights of the author of a database in the case of reproduction for private purposes of a non-electronic database. A contrariori the reproduction of an electronic database for private purposes is excluded.

28. According to article 5 (2) of the Software Directive, the lawful user has the right to make a back-up copy of the computer program and the Directive does not establish a private copy exception.

29. See for example article L-111-3 of the French Intellectual Property Code (CPI) and article 17 of the Greek Law 2121/1993.

owner. In other words, intellectual property over the work and the real property over the tangible medium shall be exercised autonomously, and in parallel without overlapping each other.

In the analog era, the status of the liberties of the owner of the medium concerning the use of the work which is integrated to the medium she owns is rather clear. The owner of a book which embodies a literary work or the owner of a CD incorporating works of music can read it or listen to it, and is entitled to make a private copy of it, if the private copy exception is permitted by national legislation.

Digital revolution has added a totally new dimension to the delimitation of the liberties of the owner of the medium as regard to the uses of the medium and of the work which is embodied to it. Since digitization permits the easier transfer of a work to a different medium, the question of space and format shifting is raised<sup>30</sup>. Except for the question of infringement of moral right that might be raised in case of degradation of the quality of the work, does it matter for the author of music if the lawful user listens to it on a mp3 player, via a CD or via streaming? Could we define or require a more specific principle of technological neutrality, which covers the right of the user to enjoy the work of mind without the limitations put by its medium?

The concept of format shifting has been mainly argued in the field of user rights, since it refers to the possibility of owners of some form of media, such as a song or a film, to convert that media from one format to another, namely an audiotape, videotape, compact disc, or DVD into an electronic file stored on a computer or the opposite<sup>31</sup>. In the US the Ninth Circuit Court of Appeals applied the "space shifting" argument in the context of the Rio device (a portable MP3 player)<sup>32</sup> and justified the space shifting as an non commercial personal use.

In Europe, the problem refers to the restrictions of the private copy exception in the digital environment due to the application of technological measures of protection. In France, the question was fiercely put in two famous cases: the "Mullholland Drive" case, where the owner of a DVD was restricted to convert the DVD to an audiotape due to technological measures of protection, and the

---

30. In the context of this article format shifting and space shifting are used as similar concepts. Space and format shifting implies copying the work in a different location or adapting and copying the work in a more convenient format.

31. <<http://www.wikipedia.org>>.

32. *Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc.*, 180 F.3d 1072, 1079 (9th Cir. 1999). However, the space shifting defense was not accepted in the following cases: *UMG v. MP3.com*, 92 F. Supp. 2d 349 (S.D.N.Y. 2000) · *A & M Records v. Napster*, 239 F. 3d. 1004 (9th Cir. 2000).



“Phil Collins” case, where the owner of a CD of the famous artist was unable to read and copy it to the hard disc of his Macintosh computer<sup>33</sup>. In both cases, the French Supreme Court rejected the argument on the existence of a user’s right to private copying<sup>34</sup> and, consequently, indirectly recognized that the owner of a medium incorporating a work does not have a right to convert this medium to another without the right holder’s consent. It is noteworthy that in France after the promulgation of Law of the 1<sup>st</sup> August 2006, a special administrative authority (the ARMT) is charged to solve this kind of disputes. In the UK the perspective of permitting format-shifting as a part of a limited private copying exception in order to legitimize current consumer activities and, to promote innovation was proposed in the past by the Gowers Review<sup>35</sup> and, more recently, by the Review of Professor Ian Hargreaves of “Intellectual Property and Growth” which was commissioned by the UK Government<sup>36</sup>.

Nonetheless, the question of space or format shifting is raised also in the sphere of the exploitation of economic rights from the point view of the right holder, who wishes to exploit a work of mind in a different format than the one she has been reserved the right to do by a contract. In the Pink Floyd/EMI case<sup>37</sup>, the famous band had questioned EMI’s entitlement to sell individual tracks, or indeed any tracks, otherwise than in the original configuration of the Pink Floyd albums. The main argument of the band was that a clause in their record contract with EMI, which referred to the question of the “artistic integrity of the albums”, prevented EMI from selling online individual songs separately from their full albums.

In this case, the question of space shifting emerged mainly in the context of the interpretation and application of the record contract, which was signed before legal downloads were available. At the same time, the contractual term about the artistic integrity of the album could be seen as an implied reference to the moral right of integrity, even if the question of protection of moral rights was not directly raised in front of the Court. By prohibiting EMI to sell the group’s songs as single tracks as downloads, both the High Court and the Court of appeal confirmed that the record company had no right to digitize and sell independently,

---

33. Cour Cass, February 28<sup>th</sup>, 2006, Revue Lamy Droit de l’immatériel, 2006/14, n°405, obs. L. Costes.

34. Cour Cass, November 27<sup>th</sup>, 2008, n°07-18778.

35. Gowers Review on Intellectual Property, November 2006, <<http://webarchive.nationalarchives.gov.uk>> <[http://www.hm-treasury.gov.uk/d/pbr06\\_gowers\\_report\\_755.pdf](http://www.hm-treasury.gov.uk/d/pbr06_gowers_report_755.pdf)>.

36. Hargreaves I., Digital Opportunity, A Review of Intellectual Property and Growth, p. 48, May 2011: <<http://www.ipo.gov.uk/ipreview-finalreport.pdf>>.

37. *Pink Floyd Music Ltd v EMI Records Ltd* [2010] EWCA Civ 1429.

thus to space shift, the group's songs without the group's specific consent. The verdict clearly demonstrates that there is no technological neutrality in copyright law as regards to the relation of the work with its medium.

In countries which follow the continental author's rights tradition, the question could have been analyzed under the specter of certain principles of interpretation of copyright contracts, such as the French principle of specialty, which requires that all the ways of exploitation that are transferred by the author must be clearly defined in the contract<sup>38</sup>.

The conversion to another medium could also be considered as a new unknown way of exploitation of the work and, consequently, be examined under the principle which permits the granting of a license for unknown types of use of works under certain conditions<sup>39</sup>. The assessment of this point has to take into consideration certain decisive factors, such as the sufficient autonomy of the new kind of use of work in regard to licensed uses<sup>40</sup>. It has to be mentioned that under the previous regime for unknown ways of exploitation, German case law and doctrine were divided as regards the question whether the conversion of vinyl discs to CDs constitutes a new unknown way of exploitation from a technical point of view<sup>41</sup>, while a similar question was raised as regards the right of the producer to com-

---

38. Article 131-3 of the French Intellectual Property Code (CPI).

39. See article L-131-6 of the French Intellectual Property Code (CPI) and article 31a of the German copyright law (Urheberrechtsgesetz, UrhG) as it was modified by the Law October 26th, 2007 (JO (Bundesgesetzblatt) 31 oct. 2007, I, n° 54, p. 2513 sq.). A new type of use within the meaning of the German Copyright Act requires the use to be a technically and commercially independent form of exploitation of the work (Bundesgerichtshof, 5 June 1985, GEMA-Vermutung I: GRUR 1986, 62). Under the previous regime of article 31 (4) the granting of licenses for types of use of work which were unknown at the time of the grant of the use was invalidated. See: Lucas-Schloetter A., *Lettre d'Allemagne, Qu'y a-t-il dans la «deuxième corbeille»?*, La loi allemande du 26 octobre 2007 relative au droit d'auteur dans la société de l'information, *Propriétés intellectuelles*, juillet 2008, n°28, p. 374. In France, principle of strict interpretation of the contract could lead to the denial of a right to convert in another format : CA Paris, 1<sup>er</sup> ch., 20 février 1981, RIDA 3/1981, p.212 (the license to commercialize the film in format 35mm and 16mm does not imply that the licensee can commercialize in the form of videotapes), decision cited by Lucas A./Lucas H.J., *Traité de la propriété littéraire et artistique*, 3e édit., Lexis Nexis Litec 2006, p. 457, n°603).

40. Lucas A./Lucas H.J., *op.cit.*, p. 456, n°602.

41. OLG Hamburg, 21 nov. 2001, *Der grüne Tisch*: ZUM 2002, 297 ·OLG Köln, 22 sept. 2000, *The Kelly Family*: ZUM 2001, 166. KG Berlin, 5 juin 2003: GRUR 2003, 1038 ·KG Berlin, 30 juill. 1999: ZUM 2000, 164. OLG Düsseldorf, 14 déc. 1999: ZUM 2001, 164.

mercialize a film in the form DVDs<sup>42</sup>. In the latter case it was decided that the exploitation of films in the form of DVD is not a new way of exploitation as regards the exploitation in the form of videotapes<sup>43</sup>.

Even though the last case could be seen as an important step towards technological neutrality, as a general rule, author protective principles attribute justifiably a remarkable importance to the medium of exploitation of the work in the field of copyright contracts.

In this context, technological neutrality is rather an exception than a rule. This is clearly affirmed by an interesting decision of the First Instance Court of Paris on 16<sup>th</sup> November 2010<sup>44</sup> in a dispute between a graphic designer and a company, specialized in Iphone software applications. The main question put in front of the Court was whether a contract of transfer of copyright over a figure named “Carl” for uses of the figure in applications for smart phones entitled the company to develop and commercialize applications based on the figure for Ipads and Ipods. According to the Court, a transfer of rights for Iphone applications does not automatically include the transfer of rights for Ipad and Ipod.

## ***2.2. The dependence of the work of mind to its way of communication***

The “shape” of the work of mind plays a significant role in the exploitation of copyright, and this applies also to the dissemination of work to the public. There, too, the principle of neutrality is deemed to be more the exception than the rule. The main issue is raised when a specific legal framework is provided by the legislator regarding a particular way of communication of works of mind to the public. In other words, the dependence of work of mind to this medium of communication is apparent, when a specific communication technology is clearly or indirectly regulated through specific legal provisions.

This is the case of cable retransmission, which is ruled by the Satellite and Cable Directive<sup>45</sup>. The very interesting German “Zattoo” case demonstrates the rejection

42. OLG München, 10 oct. 2002, Der Zauberberg, GRUR 2003, 51, 53· Bundesgerichtshof, 19 May 2005, [www.bundesgerichtshof.de](http://www.bundesgerichtshof.de), JurPC Web-Dok. 142/2005. (The exploitation of films on DVD as compared with the video exploitation does not constitute a new type of use). For the exploitation of a film in the form of videotape, see also: OLG Köln, 9 January 2009 (contracts that concern the exploitation of films made prior to 1966 do not in general cover video rights).

43. BGH, 19 May 2005, Zauberberg: GRUR 2005.

44. TGI Paris, 3<sup>e</sup> ch, 16 novembre 2010, Yann X c/ SARL AWYSE et Simon Y.

45. Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and

tion of technological neutrality on this issue. Zattoo.de offers free of charge, access to TV programs through Internet to its registered users, which are diffused by German and other European broadcasters. Technically, Zattoo receives satellite TV content, converts, which encrypts and retransmits it simultaneously via Internet to its subscribers. Zattoo received the permission to retransmit from the German public broadcasters and collecting societies, but not the consent of the right holders of the content, the film studios Warner and Universal. When the content right holders sued them, Zattoo defended by arguing that their service constitutes a cable retransmission under the section 20b of the German Copyright Act and, par consequent, it is necessary to demand only the consent of broadcasters and of the collecting societies according to section 87 para. 1 and section 20b of the German Copyright Act. In view of the fact that the network infrastructure used by Zattoo consists of interconnected cables and technically resembles the circulation via conventional coaxial cable, section 20b GCA could be understood to include also Internet retransmission. However, the Court insisted on a narrow interpretation in accordance with the historical context of section 20b and rejected this analogy despite the similarities between the technologies of retransmission. The Court also emphasized on the great potential of widespread diffusion offered by Internet compared to the more limited and more expensive one of co-axial cables and to the potential far reaching effects of the Zattoo service to content right holders<sup>46</sup>. In other words, when the legislator explicitly mentions a technology, there can't be any use of a principle of technological neutrality.

### ***2.3. Technological neutrality and the exhaustion of the right of distribution***

Technological neutrality does not simply exist in regard to the exhaustion of the distribution right, since by definition the distribution right concerns only the dissemination of the work through a tangible object.

Indeed, the principle of Community exhaustion applies only to the transfer of tangible media incorporating the work, and does not concern digital copies of the work<sup>47</sup>.

---

cable retransmission, Official Journal L 248, 06/10/1993 P. 0015 – 0021.

46. Regional Court of Hamburg, 8 April 2009, (ref. no. 308 O 660/08). For a report of the case in English see: Bird & Bird, Copyright Update, An Update of the Developments in Europe 2009, <http://www.twobirds.com/English/Publications/NewsLetters/Upload/Copyright%20Update%202009.pdf>.

47. For an analysis of the challenges to the principle of exhaustion in the digital environment, see Gaubiac Y., The exhaustion of rights in the digital environment, Copyright Bulletin, vol. XXXVI, n°4, 2002, <http://unesdoc.unesco.org/images/0013/001397/139700e.pdf>:

This is clearly affirmed by the Software<sup>48</sup>, the Database<sup>49</sup> and the Infosoc Directives<sup>50</sup>, while the same principle also applies in the US where the first digital sale doctrine was rejected by the US Copyright Office<sup>51</sup>.

The notion that the electronic distribution of works does not give rise to the exhaustion doctrine because it falls under the scope of the right of making a work available to the public, rather than under the right of distribution, is now part of the *acquis communautaire*<sup>52</sup>.

Nevertheless, the question of exhaustion becomes more complex if the right holder has given her consent for a given mode of distribution, but the licensee engaged an activity outside his limited license. This could be a case where the right holder gave his consent for the distribution of a film in form of CD, and the licensee distributed the film in form of DVDs. Are the effects of the exhaustion limited to the type of distribution to which the right holder consented<sup>53</sup>, in our case the distribution in the form of CD? And more especially is the distribution right exhausted for third parties, for example the retail sellers, who distributed the film in form of DVD after they bought it by the right holder's contractual partner? The assessment of this question demands careful consideration. In general, disregarding of content related restraints of sales channels by the contractual partner of the author may be effective and, thus, avoid exhaustion for primary transgression

---

48. Article 4 of the Software Directive (Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, Official Journal L 122, 17/05/1991 P. 0042 - 0046).

49. Article 5 (2) of the Database Directive (Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, Official Journal L 077, 27/03/1996 P. 0020 - 0028).

50. Article 4 (2) of the Infosoc Directive.

51. H.R. Rpt. No. 551 (Part 2), 105th Congress, 2d Session 24 (1998).

52. IVIR, Study on the Implementation and Effect in Member States' Laws of Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, op.cit., p. 26. According to Recital 29 of the Information Society Directive: "The question of exhaustion does not arise in the case of services and on-line services in particular. This also applies with regard to a material copy of a work or other subject matter made by a user of such a service with the consent of the right holder. Therefore, the same applies to rental and lending of the original and copies of works or other subject matter which are services by nature. Unlike CD-ROM or CD-I, where the intellectual property is incorporated in a material medium, namely an item of goods, every on-line service is in fact an act which should be subject to authorisation where the copyright or related right so provides."

53. *Bechtold*, in Dreier/Hugenholtz, Concise European Copyright Law, Kluwer Law International, 2006, p. 364.

of the contractual restraint<sup>54</sup>. The dependence of the work to its medium, thus to a given form of exploitation, seems to prevail here too, since as in the field of copyright contracts, there is a question of interpretation and effectiveness of contractual terms.

## Conclusion

The time has come to answer to the question at title of this article: Is the principle of neutrality in copyright law a myth or a reality? The principle has been used and promoted from time to time, but was never really defined or described and, by consequence, the answer depends on the way we conceive the content of this principle. If we define the principle as the general rule that copyright law applies to new technologies and extends its limits to new applications, technological neutrality of copyright law surely exists. However, if it is defined more precisely as the principle of independency of the work of mind to its medium, we have to conclude that such a principle does not really exist in copyright law.

According to McMulhan, the medium is the message, and in copyright law the medium still has a significant role, even if the official dogma is to postulate the independence of the work of mind to its medium. The digital era offers to the doctrine the challenge to operate an ideological shift in the conceptual relation between the intellectual creation and its medium of incorporation: to define the work of mind not only as an expression but as an expression engraved in a particular medium.

For, example, is it the same experience to read a book with the traditional way or with an e-book reader? In the first case, it is possible to lend the book, to open it randomly, to throw it away. In the second case, there are the functions of search, memorize, zoom, copy, delete. Is it still the same work? In some way, from a user's point of view, -and in our opinion the various ways a work is experienced by the public should not be disregarded-, the answer is no<sup>55</sup>.

While the dematerialization brought by the digital revolution could have decreased or even extinguished the dependence of the intangible work to its medium, reality shows that works of mind can be perceived and enjoyed in a totally

---

54. Walter M. and Lewinski, S. Von, European copyright law, a commentary, Oxford University Press, 2010, p. 999-1000.

55. In the US case *RealNetworks v. Streambox*, it was argued that the conversion to another format infringes the right to create a derivative work. This could be seen as an implied recognition that format shifting ends up to the creation of a new work due to the change of the technical characteristics of the work: *RealNetworks v. Streambox*, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 2000).

different way depending on the media through which they are communicated to the public. Does this mean the author's consent is necessary for every conversion of the medium to a different medium or format? The debate is open and has to be discussed in detail, since none of the existing exceptions directly provides a legal basis for this. Even it is undeniable that a paper copy of a literary work presents significant qualitative differences from the work in the digital form of e-book, this shall not be the same for the different formats of an e-book, such as the .pdf or the more and more popular ePub, which cannot be seen as qualitative dissimilar.

Apart from the answer to these emerging issues, we shall conclude as a final remark that the technological neutrality in copyright law defined as an abstract inherent vocation of every legal branch to adapt to evolutions is a reality. However, the dependence of the work to its medium mainly in the fields of copyright contracts and of exceptions, which are more and more ruled by contractual terms, is a flagrant sign that there is no such principle specific to copyright law.

# Regulation and self-regulation of online activity

## Blogs and electronic social media

---

---

Spiros Tassis

---

---

### 1. Regulating online behavior – Is it of any use?

#### *a. Do we need regulation?*

Some years ago I was asked, which is the best way to preserve freedom of speech in Internet and my answer was ... self regulation!

Indeed is common knowledge that freedom in online activity is a fundamental issue and as big as the governance of the online resources<sup>1</sup>. The typical reaction is that Internet must be free and open<sup>2</sup>. Everybody agrees this this is, probably, the last (virtual) space where everybody is able to freely express himself and many are those who actively defend this option.

The motto from the early period was going like this:

«Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather<sup>3</sup>».

What is defined, though, as regulation? Regulation is a rule, principle, or condition that governs certain procedures or behavior and in most of the times it is generated by the legislative authorities such as the parliament, the respective ministry or the relevant NRA. This intervention is formed to rules and limits in rendering or/and using the relevant sources (both scarce and not) and services. Thus, the regulation turns to form at least a base line of rules for any online activity.

- 
1. For a list of methods to oppress freedom of online speech see a relevant report by the “Committee to Protect Journalists” <<http://www.cpj.org/reports/2011/05/the-10-tools-of-online-oppressors.php>>.
  2. There are hundreds of organizations declaring that Internet means freedom of speech. As most of them say “There is no freedom of information without *Internet freedom*”.
  3. John Perry Barlow: «A Declaration of the Independence of Cyberspace». 1996. American poet, founder of the EFF and activist for the freedom of speech in Internet. He introduced the term “cyberlibertarian”.



But do we, really, need any specific regulation for online activity or should we leave the stakeholders alone to form the rules of this “sui generis” environment? The traditional legal texts are not just enough?

Studies say that only in EU more than 107 million users will be active in online social networks by the year 2012. The relevant risks are enormous<sup>4</sup>:

1. No oblivion on the Internet: The notion of oblivion does not exist on the Internet. Data, once published, may stay there literally forever - even when the data subject has deleted them.
2. The misleading notion of “community”: Many service providers claim that they are bringing communication structures from the “real” world into cyberspace.
3. “Free of charge” may in fact not be “for free”, when users of many social network services in fact “pay” through secondary use of their personal profile data by the service providers, e.g. for (targeted) marketing.
4. Traffic data collection by social network service providers, who are technically capable of recording every single move a user makes on their site; eventually sharing of personal (traffic) data (including users’ IP-addresses which can in some cases also resemble location data) with third parties (e.g. for advertising or even targeted advertising) and law enforcement agencies with less protection than in the country of origin.
5. The growing need to refinance services and to make profits may further spur the collection, processing and use of user data, when they are the only real asset of social network providers. Social network sites are not – while the term “social” may suggest otherwise – public utilities, but are run by major international players entering the market need to create and maximize profits.
6. Giving away more personal information than you think you do: For example, photos may become universal biometric identifiers within a network and even across networks. Furthermore, “social graph” functionalities popular with many social network services do reveal data about the relationships between different users.
7. Misuse of profile data by third parties: This is probably the most important threat potential for personal data contained in user profiles of social network services together with the hijacking of profiles by unauthorized third parties (id theft).

---

4. As categorized by the “International Working Group on Data Protection in Telecommunications” in its published “Report and Guidance on Privacy in Social Network Services -”Rome Memorandum” - 43rd meeting, 3-4 March 2008, Rome (Italy)”. The Working Group consists of representatives from the national data protection supervisory authorities and from international data protection organisations, as well as of independent scientists, representatives from industry and other specialists in privacy and telecommunications.

8. Use of a notoriously insecure infrastructure: These incidents include well-known service providers like Facebook, flickr, MySpace, Orkut and the German provider “StudiVZ”.

9. Existing unsolved security problems of Internet services A recent position paper by the European Network and Information Security Agency (ENISA) inter alia lists SPAM, cross site scripting, viruses and worms, spear-phishing and social network-specific phishing, infiltration of networks, profile-squatting and reputation slander through ID theft, stalking, bullying, and corporate espionage (i.e. social engineering attacks using social network services). According to ENISA, “social network aggregators” pose an additional security threat.

10. The introduction of interoperability standards and application programming interfaces (API; e.g. “open social” introduced by Google in November 2007) to make different social network services technically interoperable entails additional new risks: they allow for automatic evaluation of all social networks websites implementing this standard.

In all the above, we should add the persistent effort to minimize privacy in online activity pushed by several governmental agencies across the world, which impose pro-active control of all data, aiming to control and check information that may relate to potential criminal behavior or terrorism and, of course, the notion of monitoring the employee’s use of online services (such as the electronic social networks) during working hours<sup>5</sup>.

These efforts mean two things: first, we do need specific regulation for electronic communications, and second, regulation is not always depressing the freedom of speech. On the contrary, the appropriate regulation, very often helps users avoid serious risks and hazards to our privacy and other fundamental rights. The enemy of proportional regulation is ... over-regulation of online activity. Proportional regulation of online activity should result to protecting online privacy and promoting net neutrality.

### ***b. How much regulation?***

Regulation should intervene where users should be protected, not only from the government or the big companies, but also from other users who misuse Internet. That means regulation relevant to activities that creates a big public interest (as e.g. the online gambling, e-commerce, online financial services and protection of minors) is usually welcome and accepted - as soon it stays within the limits of respecting the human rights. On the other hand, any regulation aiming to protect an indefinite “public interest” or from generic social groups seen as “public

---

5. <<http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf>>.

enemies” is being treated with suspicion, because it simply leads to more surveillance and less privacy and overall to less respect to fundamental civil rights. This regulation often remains ineffective in practice.

***c. Basic Regulation in EU affecting online social networks and blogging***

- 1987: Commission Green Paper on the development of a common market for telecommunications services.
- 2002: EU agrees need for new regulatory package (Telecommunications Framework 2002)
- 2007: Commission presents a new telecoms ‘package’ of reforms
- 2009: A new framework for the electronic communications is created (Electronic Communications Framework 2009)

The existing 2002 regulatory framework for electronic communications networks and services in the European Union is comprised by five directives, which altogether are referred to as “the Framework Directive and the Specific Directives”. More specifically these directives are: (a) Directive 2002/19/EC of the European Parliament on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), (b) Directive 2002/20/EC of the European Parliament on the authorisation of electronic communications networks and services (Authorisation Directive), (c) Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive), (d) Directive 2002/22/EC (Universal Service Directive), and finally, (e) Directive 2002/58/EC (Directive on privacy and electronic communications). Directives 2002/22/EC and 2002/58/EC were amended by Directive 2009/136/EC and Directives 2002/19/EC, 2002/20/EC and 2002/21/EC were amended by Directive 2009/140/EC.

***d. Main elements of the new reform (valid from 25 of May 2011)<sup>6</sup>:***

Protecting citizens’ rights relating to internet access is done by a new internet freedom provision following the strong request of the European Parliament, and after long negotiations on this point. The new telecoms rules, in a new Internet freedom provision, now explicitly state that any measures taken by Member States regarding access to or use of services and applications through telecoms networks must respect the fundamental rights and freedoms of citizens, as they

---

6. <[http://ec.europa.eu/information\\_society/policy/ecomm/tomorrow/reform/index\\_en.htm](http://ec.europa.eu/information_society/policy/ecomm/tomorrow/reform/index_en.htm)>.

are guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms, and in general principles of EU law. Such measures must also be appropriate, proportionate and necessary within a democratic society. In particular, they must respect the presumption of innocence and the right to privacy. With regard to any measures of Member States taken on their Internet access (e.g. to fight child pornography or other illegal activities), citizens in the EU are entitled to a prior fair and impartial procedure, including the right to be heard, and they have a right to an effective and timely judicial review.

New guarantees for an open and more “neutral” net (Net Neutrality). Another way to hinder freedom of speech and access on certain online social networks and non-friendly bloggers is the management of the internet sources in a way to limit bandwidth capacity or direct users to friendly services. The European Commission has repeatedly declared that it “will not put the achievement of the open internet at risk. Everyone in the EU should have the chance to enjoy the benefits of an open and neutral Internet, without hidden restrictions or slower speeds than they have been promised”<sup>7</sup>. The new telecoms rules, according to the European Commission, will ensure that European consumers have an ever greater choice of competing broadband service providers. Internet service providers have powerful tools at their disposal that allow them to differentiate between the various data transmissions on the internet, such as voice or ‘peer-to-peer’ communication. That is why, under the new EU rules, national telecoms authorities will have the powers to set minimum quality levels for network transmission services so as to promote “net neutrality” and “net freedoms” for European citizens. In addition, thanks to new transparency requirements, consumers must be informed – before signing a contract – about the nature of the service to which they are subscribing, including traffic management techniques and their impact on service quality, as well as any other limitations (such as bandwidth caps or available connection speed). This is a good example on how the Internet’s economics (antitrust and unfair competition practices) may be helpful (even sideways) in supporting freedom and privacy.

Consumer protection against personal data breaches and spam European citizens’ privacy is a priority of the new telecoms rules. Names, email addresses and bank account information of the customers of telecoms and internet service providers, and especially the data about every phone call and internet session, need to be kept safe from accidentally or deliberately ending up in the wrong hands. Operators must respond to the responsibility that comes with processing and storing

---

7. Neelie Kroes European Commission Vice-President for the Digital Agenda The internet belongs to all of us Press conference on Net Neutrality Communication Brussels, 19th April 2011.

this information. Therefore, the new rules introduce mandatory notifications for personal data breaches – the first law of its kind in Europe. This means that communications providers will be obliged to inform the authorities and their customers about security breaches affecting their personal data. This will increase the incentives for better protection of personal data by providers of communications networks and services.

In addition, the rules concerning privacy and data protection are strengthened, e.g. on the use of “cookies” and similar devices. Internet users will be better informed about cookies and about what happens to their personal data, and they will find it easier to exercise control over their personal information in practice. Furthermore, internet service providers will also gain the right to protect their business and their customers through legal action against spammers. The new EU Directive 2009/136/EC regarding the use of ‘cookies’ is imposing strict rules on website providers on the way in which cookies are used. According to this Directive, website providers will need to receive explicit consent from users in order to store cookies on website users’ devices so that the website can recognize the user’s device in future. But as it became obvious the member states were not so enthusiastic about implementing these new stricter rules.

All these new elements try to provide a more secure environment for users of the online social networks and the bloggers, and, at the same time try to motivate fair competition among the operators of these services. “Europe’s competition frameworks and the EU Directives for electronic communications already guarantee the openness of Internet and transparency for consumers while recognizing the need for innovation in networks and business models. With the fast increase in data traffic over fixed and mobile network, smart management of networks is essential for offering service quality to all end-users and for developing new innovative services”<sup>8</sup>.

Two steps ahead and one beyond: On the other hand Europe recently introduced a really problematic directive regarding obligatory data retention. This new Directive (2006/24/EC) gave to many governments the opportunity to impose more privacy-free legislation, e.g. the French Government recently defined data that must be retained “at the transmission or modification of online content, by the hosting companies, including video sharing and blog hosting services allowing for the identification of any person having contributed to the creation of online content”. In Greece the mentioned Directive combined with the interpretation by

---

8. Luigi Gambardella, ETNO Executive Board Chairman <<http://pr.euractiv.com/press-release/open-internet-maintaining-openness-internet-and-supporting-new-and-innovative-business>>.

the public prosecutor of Supreme Court that the external data of communications should not be treated as confidential as the content of the communication has led to a significant increase of the police's demand for disclosure of internet related data from the operators.

## 2. Self Regulation

Regulation can cover many aspects of the online activity, but it sets only the basic principles. The details of each online service and community must be respected by all stakeholders through a self-restriction scheme.

### *a. What is Self-regulation?*

By self-regulation we define “when industry administers and enforces its own solution to address a particular issue without formal oversight or participation of the regulator or government. In particular, there is no *ex ante*, legal backstop in a self-regulatory scheme to act as the ultimate guarantor of enforcement”<sup>9</sup>. Self-regulation or self-restriction is the voluntary acceptance by all stakeholders to respect a series of norms agreed specifically for a certain online activity.

More often the self-regulation rules are set by the operator of an internet service, thus the main forms of self-regulation are the “Code of Conduct” and the “Terms of Use”. Both instruments rely on the user's good intentions to respect them and its fair use of the respective services.

[Self-regulation has also been promoted and encouraged by the legislators such as the EU through several Recommendations issued:

- Recommendation (2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), which strongly suggests the creation of principles and mechanisms concerning self-regulation and user protection against illegal or harmful content on new communications and information services by establishing Self-regulatory organizations, Content descriptors, Content selection tools, Content complaints systems, Mediation and arbitration procedures, and securing user information and awareness.
- Recommendation 2006/952/EC which calls for a further step to be taken towards establishing effective cooperation between the Member States, the industry and other interested parties regarding the protection of minors and human dignity in the broadcasting and Internet services sectors. It supplements

---

9. As defined by Ofcom at <[www.ofcom.org.uk](http://www.ofcom.org.uk)>.

Council Recommendation 98/560/EC on the same subject, taking into account recent technological developments and the changing media landscape].

### ***b. Is Self-regulation effective?***

Self-regulation always was the preferred method of online activity governance. It started in the mid 90's as the preferred mean of setting rules for online activity, and from the very beginning became apparent that if some basic rules could not followed, the self-regulation schemes would not be able to lead to an open and fair virtual world. But it is not easy to find out how effective it is unless it is tested for many years and within, certain cultural and economic environment.

Bertelsmann Foundation gave a clear answer on this question: "For a public response of Self-regulation of Internet content to be effective, it must be integrated, systematic and dynamic, sensitive to public needs and national differences within a framework that encourages robust communication. Only such a systematic approach – bringing technological potential together with the energies and capacities of government, the Internet industry and the citizenry – has the promise of success in meeting what often seem to be competing goals. Given the global and borderless architecture of the Internet, such a systematic approach requires not only coordination at a national and regional level, but its scope must be international. Codes of conduct should be adopted to ensure that Internet content and service providers act in accord with principles of social responsibility. These codes should meet community concerns and operate as an accountability system that guarantees a high level of credibility and quality. As part of the codes of conduct, Internet providers hosting content have an obligation to remove illegal content when put on notice that such content exists. The procedure for such notice and take-down – while laid down by regulation – should be reflected in codes of conduct and should specify the requirements for proper notification of service providers"<sup>10</sup>.

More than 15 years after, we are in position to tell that as long the technology is progressing and the online business is flourishing, the Internet is turning to a real battlefield for financial wars, where the self-regulation schemes turned to be inadequate and very often misused. "The concept of self-regulation is now being used in a way that extends far beyond its initial meaning to cover activities that are neither "self-" nor "regulation" but devolved enforcement, surveillance and extra-judicial punishment of allegedly illegal activities"<sup>11</sup>.

---

10. Self-regulation of Internet Content, Bertelsmann Foundation, Gütersloh 1999.

11. EDRI "The slide from self regulation to corporate censorship" <[http://www.edri.org/files/EDRI\\_selfreg\\_final\\_20110124.pdf](http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf)>.

On the other hand, it is true that being self-restricted when it comes to privacy may deteriorate your position in the market. "It costs to be proactive on privacy. Companies concerned with privacy may turn away from business practices their less principled competitors jump at, or devote significant resources to supporting self-regulatory or technical programs. Regulatory actions (self or statutory) are not cheap. The cost of privacy when placed in the broader context of user satisfaction, fraud reduction, and user confidence in the Web is worthwhile, however the cost is uncertain and poorly distributed"<sup>12</sup>.

### *c. Terms of Use (or Terms and Conditions) as self-regulation schemes*

Online social networks and blogging services providers have implemented the majority of the regulatory principles in their terms of use. As a user you cannot join in without have agreed to these terms and conditions which are a take-it-or-leave-it legal document.

"One cannot go online today without eventually being asked to accept a set of so-called Terms of Service (or TOS). These "terms" are actually purported legal contracts between the user and the online service provider despite the fact that users never get a chance to negotiate their contents and can often be entirely unaware of their existence. In the unregulated and unpredictable world of the Internet, such arrangements often provide the necessary ground rules for how various online services should be used. Yet TOS agreements also raise a number of concerns for the consumer, as they can be a vehicle for abuse by online service providers, as they tend to end up being one-sided in the service provider's favor, and are often designed to be beyond any judicial scrutiny"<sup>13</sup>.

- Users of "blogger.com" are obliged to accept several terms regarding fair use of the service: "Proper Use ... the user agrees that he will use the Service in compliance with all applicable local, state, national, and international laws, rules and regulations, including any laws regarding the transmission of technical data exported from your country of residence and all United States export control laws ... By their very nature, Blogger.com and Blogspot.com may carry offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are otherwise deceptive. We expect that you will use caution and common sense and exercise proper judgment when using Blogger.com and Blogspot.com.

---

12. Joseph M. Reagle Jr. reagle@mit.edu, Resident Fellow, Berkman Center for Internet & Society, Harvard Law School, <[http://cyber.law.harvard.edu/archived\\_content/people/reagle/privacy-selfreg.html](http://cyber.law.harvard.edu/archived_content/people/reagle/privacy-selfreg.html)>.

13. <<http://www.eff.org/issues/terms-of-abuse>>.



Google does not endorse, support, represent or guarantee the truthfulness, accuracy, or reliability of any communications posted via the Service or endorses any opinions expressed via the Service. You acknowledge that any reliance on material posted via the Service will be at your own risk.

Content Boundaries means that no adult content is allowed on Blogger, including images or videos that contain nudity or sexual activity and that Blogger has a zero tolerance policy towards content that exploits children. In addition other content not allowed is hate speech, crude content, violence, copyright infringement, disclosure of Personal and confidential information especially when these belongs to third parties, impersonating others, illegal activities (for example, encouraging people to drink and drive), spam, malware and viruses.”

- Facebook declares and obliges users to declare, among others, that:
  - “You will not post content or take any action on Facebook that infringes or violates someone else’s rights or otherwise violates the law.
  - We can remove any content or information you post on Facebook if we believe that it violates this Statement.
  - If we remove your content for infringing someone else’s copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal.
  - If you repeatedly infringe other people’s intellectual property rights, we will disable your account when appropriate.
  - If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.
  - You will not post anyone’s identification documents or sensitive financial information on Facebook.
  - You will not tag users or send email invitations to non-users without their consent.
  - You will not send or otherwise post unauthorized commercial communications (such as spam) on Facebook.
  - You will not collect users’ content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission.
  - You will not bully, intimidate, or harass any user.

- You will not post content that: is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
- You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory”.

Now, seriously, does anyone believe that all users of these services do respect the above terms? As we have demonstrated these rules are breached many times by the users. Online bullying occurs often in social networks and the same applies with sharing or publishing not authorized content (IP protected, photos of persons with no consent etc.). Needless to mention that recent studies have revealed that some pedophiles have found a home for social networking on Facebook, where they can securely exchange their hideous content covered by the way the user groups are treated<sup>14</sup>. But Facebook assumes no legal responsibility for child pornography, according to Mexican journalist Lydia Cacho<sup>15</sup>, which was the one to reveal that “when [Facebook] finds a page containing images of child pornography, it closes the account. The problem is that once the account is closed, it wipes away all traces of the user and any evidence that police could have used to prosecute him or her. In addition, she says, the user often opens a new Facebook page with the same content within a day”.

How the Facebook reacted on these accusations? According to the same source ([www.baycitizen.org](http://www.baycitizen.org)) “it had taken down the journalist’s own Facebook page after she denounced those who post child pornography on Facebook. In response to that claim, Wolens wrote: “We will not comment on specific profiles for privacy reasons, however, we will disable any account found violation our Statement of Rights and Responsibilities”.

And this is not the sole case where providers of such online services are using their Terms and Conditions in order to - suspiciously - ban organizations, groups or people. Facebook (again) recently took down 50 activist groups’ accounts in UK for alleged breaches of the Terms and Conditions<sup>16</sup>. The problem with the industry self-regulation schemes is the fact that it is so difficult for commercial companies, implemented in online business, to be fair in balancing privacy with

---

14. <<http://www.foxnews.com/scitech/2010/09/28/pedophiles-find-home-social-networking-facebook/>>.

15. Mexican journalist Lydia Cacho has taken on some of the most powerful figures in Mexico, from businessmen to politicians, who have colluded with child pornography rings. Now the womens rights crusader is going after a Bay Area-based company that she says is allowing sexual predators to operate with impunity: Facebook <<http://www.baycitizen.org/blogs/pulse-of-the-bay/anti-child-pornography-crusader-takes/>>.

16. <[http://wiki.openrightsgroup.org/wiki/FB\\_takedowns](http://wiki.openrightsgroup.org/wiki/FB_takedowns)>.

practices as spam and government pressure that eventually they step back. That is why the self-regulatory schemes and dispute resolution procedures established by service providers are, often, seen such as prejudiced and suspicious. Because, really, who wants a big corporation as Facebook and Google to judge whether his account will be blocked or his data will be disclosed to the authorities based only on an alleged “breach” of the accepted (?) terms and conditions? And how many of us do firmly believe that all personal data stored in the servers of these providers are secured and not disclosed, mined or sold? “It’s easy for us to imagine that laws and public pressure can hold corporations in check, and, therefore, this is the most important thing to do. In practice, holding corporations to account is very difficult, and power relations tend to hold the day<sup>17</sup>”.

#### ***d. Is self-regulation still an option?***

This continuous battle for governance of the Internet and the variety of the stakeholders involved led to a situation in which “the Internet is de facto co-regulated by National Governments - that intervene, however, without strongly co-ordinating among themselves - by professional entities - whose competencies overlap and which are not always legitimate - and instances of technical standardization - that are very dynamic, but that lack strong institutional roots. This present institutional framework is problematic for at least two reasons: it is partly inefficient in the sense that there are incompletenesses, conflicts and defaults in enforcement in the set of implemented rules; and the current processes used to establish these rules do not guarantee that the interests of all the stakeholders are fairly taken into account”<sup>18</sup>.

All the above must have made Robert Madelin (Director General for the Information Society and Media) to state that “*self-regulation is coming under enormous scrutiny. Proof it can work needs to be brought to ripeness quickly*”<sup>19</sup>.” According to Madelin, self-regulation in order to succeed it must be founded on three basic principles:

1. Transparency. All stakeholders must be involved from the start
2. Accountability. All the parties must set goals and agree the principles
3. Monitoring. Agreed metrics are vital

---

17. <<http://www.openrightsgroup.org/blog/2011/corporations-may-not-protect-your-free-speech-and-privacy>>.

18. Open Internet - Maintaining the openness of the Internet and supporting new and innovative business models to foster network development published by ETNO <[www.etno.org](http://www.etno.org)> on Tuesday 19 Apr 2011.

19. Speech on the 16th March, 2011. Crowne Plaza Hotel. Brussels.

## Conclusions

Freedom in Internet, and especially when it comes to social networks and blogging, is still essential and a prerequisite for the existence of the internet. After so many years though we have seen that the old days when the online community was self-restricted and inspired by the pure ones (as the “cyberlibertarians” dreamed about) have long passed and gone. Even their successors “cyberutopians” cannot rigidly justify that having no regulation is the right answer even when we are talking about how the social media conveys the message (and the messages) for a revolution, as it happened recently in Arab countries. The “cyberutopians” support the idea (and actually seem to believe) that repressive regimes can be overturned in social media and networks. But I would have to agree with the statement *“the Internet is neither necessary nor sufficient for a revolution. An outraged and unified population is both”*<sup>20</sup>.

Nowadays, the online community services are owned by multinational companies aiming to gain more profit. On the other hand, it is usual that the users of such services cannot understand the risk on their privacy and the impact their online activity may have on their real life. *“In EU a quarter of children on social networking sites say they have their profile open to public. One fifth of children whose profile is public say this profile displays their address and/or phone number. In 15 out of 25 countries, 9-12 year olds are more likely than 13-17 year olds to have public profiles. Only 56% of 11-12 year olds say they know how to change privacy settings on their social network profile. Older youngsters have better skills with 78% of 15-16 year olds saying they know how to change their privacy settings”*<sup>21</sup>.

Additional risks that children and teenagers will probably face, include grooming (where adults can pass for young people with the intent of abusing children), accidentally finding inappropriate content and abuse of personal or private information and cyber-bullying.

Therefore, children and teenagers need to learn how to be empowered, they need to manage their online identity in a responsible way by using the privacy settings offered by social networking services, selecting friends online that they can trust, publishing their own photos after thinking carefully about the potential consequences, and pictures of their friends with their permission<sup>22</sup>.

---

20. “Of cyber-skeptics and cyber-utopians – debunking myths and discussing the future” <<http://www.meta-activism.org/>>.

21. Digital Agenda: children using social networks at a younger age; many unaware of basic privacy risks, says survey Reference: IP/11/479 Date: 18/04/2011.

22. <<http://ec.europa.eu/saferinternet>>.

We have to deal properly and with responsibility with the social networking sites and blogging services because these new services have changed the way we communicate and, of course, they have forced the introduction of new technologies to all age groups, and especially the youngsters. As Evgeny Morozov says "Social media – by the very virtue of being "social" – lends itself to glib, pundit-style overestimations of its own importance. In 1989, the fax-machine industry didn't employ an army of lobbyists – and fax users didn't feel the same level of attachment to these clunky machines as today's Facebook users feel toward their all-powerful social network"<sup>23</sup>.

It is true that blogging has given voice to people and has allowed many of them to shout out their beliefs and ideas, the chance to express their self and, consequently, a part of their generation. We must realize, though, that all these are happening in an era in which the perception of innocence it is not as it used to be. Childhood and social activity, even in the real world, are not as they used to be. Adolescent happens earlier and ends very soon. The electronic social media have changed the way we make friends, the way we socialize the way we find a job and have a career. At the same time, being a member of such a community is far less innocent than being with the gang of school mates. Now our intimate thoughts can be permanently stored and revealed, accidentally or not, to people, and in time totally out of our control.

Blogging, which supposedly transfers the unbiased voice of some people, may often be used for hidden commercial and competition wars and secret public policy. All these simply mean that the defending freedom and anonymity of bloggers has, also, a side effect; semi-colon the lack of any control on postings notwithstanding the fact that often the impact of such online activity is that some people are losing their jobs, their friends or even their lives due to a blog posting or a careless conduct in online social networks. We have to make sure that there is adequate regulation in order to safeguard privacy and free expression and, at the same time, keep the online environment as safe as it needs. Social networks should - ideally - provide sociability. Blogging should mean the sharing of ideas and notions. We have to make sure that all legal instruments used aims towards this target.

The lack of regulation cannot be the right way, for a democratic society, in addressing the social effects of this new social phenomenon. We cannot let the creation of a chaotic world just to preserve an undefined and unlimited freedom. As

---

23. In its Article "Facebook and Twitter are just places revolutionaries go" published online <<http://www.guardian.co.uk/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians>>.

Morozov says “what if the liberating potential of the Internet also contains the seeds of depoliticization and thus dedemocratization?”<sup>24</sup>

The bigger the virtual world becomes the less the private space remains to individuals. The bigger the financial and political stakes implemented the less we can expect a– voluntarily – fair usage of Internet resources. We need both regulation and self-regulation, but in quantities able to make them comprehensive and acceptable. Regulation can succeed when it does not lift barriers. Self-regulation can work as long as it is broadly accepted by stakeholders and provide for effective enforcement. These two vehicles may be combined and create other appropriate means of administering this virtual world and the conflicting powers. The most prominent of these new vehicles seems to be the co-regulation. The co-regulation schemes are an extension of self-regulation that involves both industry and the government (or regulator) are administering and enforcing a solution in a variety of combinations. “Thus the aim is to harness the benefits of self-regulation in circumstances where some oversight may still be required”<sup>25</sup>.

Convergence is creating a new environment where users will be able to traffic their data in several communications markets at once. This kind of use of social media will be a necessity as these services improve and mingle with cloud computing and remote access facilities. Regulation turns to be crucial once again, and that is a reality we need to accept and go forward by being careful but productive on the formulation of the regulation and the preservation of all these fundamental citizen rights that exist in Europe for decades. “As a platform for free expression, for community, for business Internet may even be our most valuable communal asset. For that reason the internet must be managed carefully, transparently and lightly”<sup>26</sup>. We need to create a new generation of e-citizens that will be inspired by the traditional elements of respect and fairness. We need to convey these old principles to the new promise land.

---

24. Morozov Ev. (2011), «The net delusion: the dark side of internet freedom», public affairs (January 4).

25. A consultation proposing an incentive-based approach to self- and co-regulation in UK communications <[www.ofcom.org.uk](http://www.ofcom.org.uk)>.

26. Neelie Kroes, European Commission Vice-President for the Digital Agenda “The internet belongs to all of us Press conference on Net Neutrality Communication” Brussels, 19th April 2011.

# **Beyond the boundaries of open, closed and pirate archives: lessons from a hybrid approach**

---

**Prodromos Tsiavos &  
Petros Stefaneas**

---

## **1. Introduction**

The emergence of digital networked archives has marked the advent of a new era for the archive and its relationship both with memory institutions and content providers. Whereas, archives have traditionally operated as organisations responsible for the preservation and controlled access to content with a limited impact upon its regular, commercial dissemination and exploitation, the digitisation of the archives, first, and their availability over digital networks, subsequently, has substantially changed their role and impact (Bernstein 2008). In a rather ironical fashion, archives seem to be the victims of their own success. We need to further elaborate on this position.

The digitisation of the material contained in archives and -most importantly- their digital cataloguing and curation has made archives more accessible than ever before. This practically means that the user has the ability to access the content of an archive in a much faster and easy way than in the past, to accurately identify the kind of material she wishes to access and to explore similar content in a more effective and efficient way. For as long as digital archives remained confined within the walls of their traditional institutional role and physical location, their function remained to a great extent similar to the one they had ever since their inception. However, once the archive became available over digital networks, its nature and boundaries have known a substantial transformation and expansion. Once the archival content becomes available over the public internet, a series of social, economic and legal questions emerge (Dietz 1998). For instance, is such an archive in direct competition with the owners of the Intellectual Property Rights over the relevant content?

Similar questions are further amplified by three increasingly important new types of archives, that is, commercial, open and pirate archives. Commercial archives have increased in importance since they represent a new mode of exploitation for previously not widely available material. Commercial archives seem to compete with traditional archives and are possibly disincentivised to make their material

available to an archive because of negative potential implications for their business model (Creative Archive Licence Group 2006). This becomes very relevant in cases where the archive holds valuable information sources, such as audiovisual material, newspapers or recordings of various kinds. Interestingly, even when the material is not protected under copyright any more may still have access controls based on physical property and the question to which such technical and contractual means may be used in order to restrict and control access is one of the questions explored in this paper.

Open archives are the ones where the content is made available through an open licensing scheme, i.e. when downloading, copying, further use and dissemination of the content in its original or altered form, remains free of any restrictions. In practice, open archives are placed in a spectrum of openness with respect both to the content and its metadata. Such spectrum covers from full openness, where no restrictions are posed to either content or metadata with respect to their potential uses. One aspect of openness also includes the ability of the user to add content or metadata which are then shared with different degrees of openness (Samis 2008). Pirate archiving is a trend appearing along the emergence of closed peer-to-peer networks. These make extensive use of content for which copyrights have not been cleared, however, the curation of the material is being done by the users of the network and is often superior to the quality of documentation found in regular archives (Bansal, Keller et al. 2006).

This paper explores these three types of archives and the ways in which their features could be combined in order to design a national archival policy for countries that are not net exporters of Intellectual Property Rights, such as Greece, in order to make the most out of the use of open archives. We argue that while open archives in their pure form are not always easy to create or sustain, primarily due to the ways in which the existing legal system operates, it is possible to create hybrid forms of archives with variable degrees of openness that could contribute to the cultivation of an ecology of open archives.

## **2. Research Design and Methodology**

In order to explore the ways in which hybrid archives operate, we need to use an analytical tool that explores the way value of different types is produced in cases of different archives. This value is not necessarily monetary. It could be e.g. social or other. Value is produced through the flows of content or data which is accordingly regulated by technological and/or legal means.



## 2.1 Basic concepts

The methodology employed in this report is based on the identification and analysis of three basic variables that appear in each of the case studies. These variables are as follows: (a) Value (b) Content (c) Rights. Value, content and rights are closely interrelated and it is useful to trace their relationship, as it sets the management framework for any e-content project (Young 2005; Pasquale 2006).

## 2.2 Data collection and research design

The above approach is applied in the following case studies:

(a) BlueGreece Torrent Tracker (b) BBC Creative Archive (c) Internet Archive (d) Broadcasting Archives (e) British Library Archives (f) BBC CenturyShare Project (g) British Library Archival Sound Recordings (BL ASR I and II) (h) National Library for Health eLearning Object Repository (NLH LOR) (I) Great Britain Historical Geographic Information System/ Vision of Britain Through Time<sup>1</sup>. In each of the cases we explore the ways in which this analytical scheme may give us some insight as to how licensing schemes may be used in order to produce different types of value.

## 3. Case Studies

In this section we present a series of examples of archives to highlight the different types of organization, types of material and business models.

### 3.1 Case One: BlueGreece Torrent Tracker

#### 3.1.1 Background

Blue Greece<sup>2</sup> is a private torrent tracker that has been in operation since early 2005. It numbers 37,683 active torrents and 54,782 members. Its most popular file has been downloaded 17,416 times and there are 441 seeders for the most popular item. The administrators of the site have issued a statement where they disclaim any responsibility over the content exchanged over the servers and there is an explicit statement as to how users should not use the site to download or use material when they do not have the rights to do so. Almost

- 
1. Seven of these cases are presented in this version of the paper. The NLH LOR and the GB VoB cases can be found in the full electronic version of the paper at <http://conferences.ionio.gr/icil2011>.
  2. The name of the torrent tracker has been purposefully altered so that is not directly identifiable. This is an action taken in order to ensure that the risk of prosecution for the tracker administrators as a result of this research is reduced.

the entirety of the content is copyrighted and not licensed to be re-distributed among the users. Since the site is a tracker and the files are directly exchanged between the members of the tracker, the administrators claim they have no responsibility over any copyright infringement taking place. In practice, the site is used for the illegal sharing of copyrighted content and is hence a pirate archive. The archival nature of the site is supported by the rich curation of the material, the existence of formal requirements as to how it is to be shared and distributed and the penalties in existence when these rules are not followed. It is also important to note that the types of the content found on the tracker also contains the diamond category under which very well curated or very popular material is placed.

### **3.1.2 Key content features**

- Multiple types of works (audio, video, image, text, databases)
- Mostly copyrighted material but also self-published/end-user material
- Mainly copyrights and related rights/database rights
- Extensive documentation and curation of the content

### **3.1.3 Copyright status and other rights issues**

- no copyrights are cleared
- Users create a great deal of meta-content for which there is no clear flow of rights or permissions. The value of this meta-content is effectively enjoyed by the community but is in the hands of the torrent tracker administrators that operate as custodians. This is in line with the technical nature of the medium that is fully decentralised with the indexing services hosted by the administrators and the users providing both content and meta-content.

### **3.1.4 Terms of access and use**

- Content and meta-data are fully accessible and downloadable by all registered users. Registration opens at non-prespecified times in order to control the number and influx of users. The limited amount of users allows a more filtered participation and the smooth operation of the community.
- The user must respect the netiquette of the forum and to share content in order to have a positive ratio (more than 1.0). This is done in order to increase the circulation of the material and decrease the phenomenon of hit and run or leeching or free riding of the common resource, that is the bandwidth and the actual content.

## 3.2 Case Two: BBC Creative Archive

### 3.2.1 Background

The BBC Creative Archive pilot ended in 2006 after temporarily releasing more than 500 pieces of digital content under Creative Archive Licence (CAL) draft scheme (Creative Archive Licence Group 2006). The project was set up in 2005 by the BBC, BFI (British Film Institute), Channel 4 and the Open University to make certain archive content available for the public to use under CAL. Currently the BFI and the Open University are making archive film clips available for public use under this scheme.

### 3.2.2 Key content features

- Audiovisual content
- Copyright and related rights

### 3.2.3 Copyright status and other rights issues

- All rights have been cleared by the BBC
- Content with minimal copyright problems were primarily selected, such as factual documentaries where no music score has been used.

### 3.2.4 Terms of access and use

The five basic rules of CAL can be summarized as follows<sup>3</sup>:

#### *A. Non-commercial*

Anything you create using the available content must be for your own non-commercial use. This means that you can share it freely with family and friends and use the content for educational purposes. You may not, however, sell or profit financially in any way from the use of the content, for example, artists cannot charge admission fees to exhibit work they have produced with the content.

#### *B. Share-Alike*

You are welcome to share the works (we call them ‘Derivative Works’) you produce with this content. If you do want to share your Derivative Works, please make sure you do so under the terms of the Creative Archive License, and make sure you ‘credit’ all creators and contributors whose content is included in the Derivative Works.

---

3. <http://www.bbc.co.uk/creativearchive/>.

### *C. Crediting (Attribution)*

This is your chance to make sure everyone knows what you have done, but you also need to make sure that others who have contributed to a work (a Derivative Work) are credited too. It's up to you how creatively you acknowledge others' contributions!

### *D. No Endorsement and No derogatory use*

We want you to get creative with the content we have made available for you but please do not use it for endorsement, campaigning, defamatory or derogatory purposes.

### *E. UK*

The Creative Archive content is made available to internet users for use within the UK.

## **3.3 Case Three: Internet Archive**

### **3.3.1 Background**

The Internet Archive<sup>4</sup> is a non-profit organization that was founded in 1996 to build an Internet library. Its main initial goal was to offer permanent access for researchers, historians, scholars, people with disabilities, and the general public, to historical collections that exist in digital format. In late 1999, the organization started to grow to include more well-rounded collections.

### **3.3.2 Key content features**

Now the Internet Archive includes texts, audio, moving images, and software as well as archived web pages in its collections, and provides specialized services for adaptive reading and information access for the blind and other persons with disabilities. The content of the Collections comes from around the world and from many different sectors. It may contain information that might be deemed offensive, disturbing, pornographic, racist, sexist, bizarre, misleading, fraudulent or otherwise objectionable.

### **3.3.3 Copyright status and other rights issues**

The Archive does not guarantee or warrant that the content available in the Collections is accurate, complete, non-infringing or legally accessible in user's jurisdiction. The Archive makes no warranty of any kind, either express or implied. However, the Internet Archive respects intellectual property rights and other pro-

---

4. <http://www.archive.org>.

prietary rights of others. The Internet Archive may, in appropriate circumstances and at its discretion, remove certain content or disable access to content that appears to infringe the copyright or other intellectual property rights of others.

### 3.3.4 Terms of access and use

The Archive, at its sole discretion, may provide the user with a password to access certain Collections. The Internet Archive is committed to making its constantly growing collection of Web pages and other forms of digital content (the “Collections”) freely (“at no cost”) available to researchers, historians, scholars, and others (“Researchers”) for purposes of benefit to the public.

A great part of the Internet Archive is made available to the end user under the six Creative Commons licences

## 3.4 Case Four: *Broadcasting Archives (BBC)*

### 3.4.1 Background

It is the main archive by the BBC part of which is made available online only to the UK users.

### 3.4.2 Key content features

BBC Archives<sup>5</sup> contain about 4 million items for television and radio. That is equivalent to 600,000 hours of television content and about 350,000 hours of radio. BBC Archives also have a New Media archive, which is keeping a record of the content on the BBC’s websites, a large sheet-music collection, and commercial music collections. It also contains press cuttings going back 40 years and other kinds of items. BBC records and keeps everything for a minimum of five years. After this five years period all the news, the drama, the entertainment, the high value and expensive to make programs are kept following the BBC Archives selection policy.

### 3.4.3 Copyright status and other rights issues

Due to rights’ restrictions some of the programmes in the BBC Archive Collections are only viewable from within the UK. The current agreement with copyrights holders allows the BBC Archive to stream programmes, so they can only be watched via the Archives’ website. Finally, the Archives have a well organized policy to let a user know when a programme may include content unsuitable for children or when it may be harmful to view.

---

5. <http://www.bbc.co.uk/archive/>

### **3.4.4 Terms of access and use**

Users are not allowed to free copies of programmes via the website, even if the programmes are already available to view on the website. If a programme has been broadcast within the last seven days, it may be available via BBC iPlayer. A special service, via the BBC Active, has been designed to fulfil the needs for academic and corporate training. BBC Active started as part of BBC Schools Radio in 1929. It was originally set up to produce simple teachers' notes to support the use of radio programmes in the classroom. It now publishes an extensive range of interactive resources based on BBC content, which support teaching and learning in primary and secondary schools, adult language learning and English language learning. In 2005 a joint venture was formed with Pearson to further develop these resources.

## **3.5 Case Five: British Library Archives**

### **3.5.1 Background**

The British Library (BL) is a non-departmental public body sponsored by the Department for Culture, Media and Sport of the United Kingdom. It is the national library of the United Kingdom and one of the largest libraries in the world.

### **3.5.2 Key content features**

As a legal deposit library, it receives copies of all books produced in the United Kingdom and the Republic of Ireland. Its collection includes well over 150 million items, in most known languages. It receives 3 million new items every year. The British Library Collections consist of manuscripts, maps, newspapers, prints and drawings, music scores and patents. The Sound Archive keeps sound recordings from 19<sup>th</sup> century cylinders to CD, DVD and MD recordings. The Library's collections include around 14 million books along with substantial holdings of manuscripts and historical items dating back as far as 2000 BC. British Library operates the world's largest document delivery service providing millions of items a year to customers all over the world.<sup>6</sup>

### **3.5.3 Copyright status and other rights issues**

The content (content being images, text, sound and video files, programs and scripts) of the BL website is copyright © The British Library Board. All rights expressly reserved. The users have to agree to abide by all copyright notices and restrictions attached to the content and not to remove or alter any such notice or restriction.

---

6. Online catalogues, information and exhibitions can be found on BL website [www.bl.uk](http://www.bl.uk).

### 3.5.4 Terms of access and use

The content of the BL website can be accessed, printed and downloaded in an unaltered form (altered including being stretched, compressed, coloured or altered in any way so as to distort content from its original proportions or format) with copyright acknowledged, on a temporary basis for personal study that is not for a direct or indirect commercial use and any non-commercial use.

## 3.6 Case Six: *BBC CenturyShare Project*

### 3.6.1 Background

The BBC CenturyShare project is jointly funded by JISC and the BBC Future Media and Technology (FMT), which is responsible for BBC's digital presence. The CenturyShare project is based on 'find, play and share', which is one of the BBC's Future Media and Technology strategies. The idea is to (a) find BBC's content whether it is on or off the site (b) play – or enjoy – it and (c) share it to send it someone else, so that someone else finds it and the circle starts again. This project builds on the concept of liaising with different partners to produce products on the basis of the content that all collaborating organisations have, which is consistent with the key objectives of the SCA in promoting interoperability between and across different cultural sectors. For instance, instead of user-generated content the intention is to use the assets of the partners of the SCA, focused on specific themes, and gather them into one place to give people a way into the collections without going to the owners of them directly. The project is a proof of concept to determine whether it is a viable concept for SCA partners aiming to analyse, aggregate and augment cultural content. Ultimately, content will be displayed on a timeline, so part of the activity will be taking the material and seeing if there is a date description and then adding more to the description or more keywords etc. The CenturyShare project is of particular interest as it operates in two layers: (a) it provides content collected from a network of providers and (b) it allows the collection of meta-content created by the users.

### 3.6.2 Key content features

- Multiple types of content: images, video, audio, documents (literary works), diagrams (graphical works) and compilations of content
- Multiple sources of content under different licensing schemes

### 3.6.3 Copyright status and other rights issues

- Ownership of content will remain with the originating organisation of the content

- The responsibility for the clearance of content is managed by the participant organisations
- BBC acquires licences for the user-generated content
- Data protection issues are thoroughly covered by the registration service agreement

### 3.6.4 Terms of access and use

BBC CenturyShare only provides a link to the e-content that is directly made available and licensed to the end-user by the organisation that owns the content.<sup>7</sup>

Metadata produced by the end-users are licensed to the BBC

## 3.7 Case Seven: *British Library Archival Sound Recordings (BL ASR I and II)*<sup>8</sup>

### 3.7.1 Background

The British Library's Archival Sound Recordings projects aim to digitise and make freely available 8,000 hours of digitised audio to the Higher and Further Education (HE/FE) communities of the UK. The projects are funded by JISC under its Digitisation programme. The core objectives of the project are to provide audio material for teaching, learning and research within various subject areas from history to ethnomusicology to science, across the broad range of HE/FE within a password-protected domain.

### 3.7.2 Key content features

- Multiple types of recordings: (a) unpublished recordings (b) published commercial recordings (c) oral history (d) field recordings (sound scapes)
- Multiple types of works (published and unpublished) exist such as: (a) performances (b) recorded literary works (c) sound recordings (d) musical works
- Multiple types of rights: (a) copyrights; (b) trademarks (on the brands of e.g. record companies) (c) personal data (e.g. in an oral history recording)

---

7. The BBC CenturyShare was a pilot that never managed to be fully implemented. Instead, the MemoryShare project is currently up and running that does not use content solely from the SCA partners. For an example of a memory (Amy Winehouse's death) see [http://www.bbc.co.uk/dna/memoryshare/A86333330?s\\_fromSearch=ArticleSearch%3Fcontenttype%3D-1%26phrase%3D\\_memory%26show%3D8](http://www.bbc.co.uk/dna/memoryshare/A86333330?s_fromSearch=ArticleSearch%3Fcontenttype%3D-1%26phrase%3D_memory%26show%3D8).

8. The British Library is one of the SCA sponsor organisations.



### 3.7.3 Value gains

- Educational and research value from making various forms of sound recordings freely available to the research community
- Cultural value from the preservation and dissemination of culturally important content that has not been previously published
- Increasing the visibility of the British Library archive and attracting a greater audience
- Allowing researchers to built upon primary material that is now made easily available

### 3.7.4 Rights ownership and obtained permissions

Rights are either owned by the British Library or effort is invested to obtain licences from the rights holders. The multiple layers of rights existing in each work often cause severe clearance problems and result in the emergence of a whole class of works without an identifiable owner (orphan works). More specifically:

- Clearance costs are high and unpredictable
- The clearance procedure affects the management of the whole project
- Clearance of rights is important not merely because of the legal liability risks but also in order to maintain the good reputation of the British Library

### 3.7.5 Terms of access and use

The content is made available to the public under two types of agreement, one for the general public and another specifically for HE/FE institutions.

- The material made available to the general public is licensed under a standard BL licence allowing end-users to copy the material for private, non-commercial and educational or research purposes. The licence does not permit adaptations or further dissemination of the work<sup>9</sup>
- The material that is made available to HE/FE institutions is licensed through the Archival Sound Recordings Sub-licence Agreement. Such a sub-licence allows under very specific conditions the copying and the limited distribution and adaptation of the content. More specifically:
  - The circulation of the licensed content is allowed but only over a secure network, such as Athens, in the UK and between specific categories of users, as described

---

9. [www.bl.uk/copyrightstatement.html](http://www.bl.uk/copyrightstatement.html)

in the sub-licence agreement. Authorised users are members of staff and students of the HE/FE institutions only

- The sub-licence allows only educational and non-commercial uses of the licensed content.
- Authorised users, as defined in the sub-licence, are allowed to incorporate parts of the licensed content in their own work provided they properly attribute the right-owners and acknowledge the source.
- Public performance of the licensed content is only possible to the extent that the relevant additional licence has been provided by the relevant collecting society

## 4. Models of permission and content flows

### 4.1 *General observations*

Different IPR management approaches appearing in the projects examined in the seven case studies may be abstracted in three main models of works and permission flows.<sup>10</sup>

Flows of permissions related to moral rights do not appear in the diagrams. This is because in all cases examined in this report moral rights remain with the creator of the content.

Three models of content and permissions flows are presented in this section. Each model is named after the key characteristic of the way in which the flows are structured. The three models are as follows:

The ‘Star-Shaped’ model

The ‘Snow-Flake’ model

The ‘Clean Hands’ model

Such models are illustrative of the ways in which IPR management may enable or hinder the flow of e-content. They also constitute a basic typology of the ways in which different models of IPR management could facilitate different types of value production. Finally, each model may be associated with different organisa-

---

10. We use the term ‘permission flows’ to denote flows of copyright licences between different users and stakeholders in each of the models. A flow does not necessarily mean that the licensor is stripped of all their copyrights. In most cases, the copyright owner only awards a licence, i.e. a set of permissions, that flows within the boundaries of the project. The exact terms and types of licences are presented in greater detail in the appendices of this report. The concept of permission mainly refers to licences, but it is broader than mere licensing. For example, in the case of the NEN Repurpose project, permissions are sought from the parents for the use of the works of their children.

tional objectives. In that sense, such models could inform the way in which IPR policy and strategy are formed.

There is no one-to-one correspondence between models and projects. For example, in each project more than one model may appear and one flow model may be used in more than one project.

## 4.2 The ‘Star-Shaped’ model

The Star-Shaped model may be applied to collections and dissemination of permissions and content.

### 4.2.1 Collection of content and permissions

The star-shaped model involves a central entity that is responsible for the acquisition of the content and the required licences from the content providers and/or other rights holders, both of whom may be individuals, organisations or other projects.

The central entity that resides at the centre of the star is the one responsible both for the clearance of the rights and the curation of the material. The flows of permissions and works follow the same direction, although they can follow different paths, i.e. flowing from the supplier to the central entity. This is because it is likely that the rights owner and the content provider may be different, and the supply of each may be made at different times, particularly when rights are cleared for legacy material already owned by the central entity. This means that the acquisition of permissions may follow a push or pull model, i.e. either the central entity is in possession of the content and asks the relevant permissions from the rights holder or the rights holder deposits the material with the central entity agreeing to license the work under specific terms and conditions set by the central entity (see Diagram I).

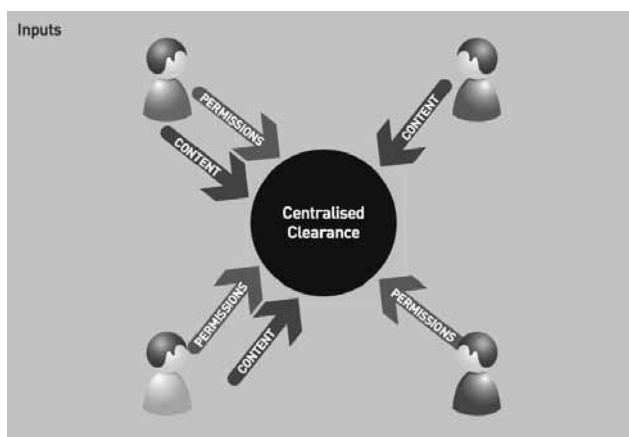


Diagram I

### 4.2.2 Impact

Most projects involving digitisation of analogue material, particularly in the context of museums and archives, are organised using the star-shaped model.

The star-shaped model reduces risks from copyright infringement as the process of copyright clearance is managed at a single point. At the same time, the cost for the organisation managing the process increases, as such a model requires a specialised service or unit to perform the function. As a result, this is a model that could be beneficial for a large organisation that can achieve economies of scale, but may not be sustainable for small and medium size organisations. In the latter case, a star-shaped model may lead the organisation to a strategy of avoiding digitisation of works that require any copyright clearance in order to reduce costs.

An organisation aiming to benefit from such a model, must establish standardised clearance processes and risk management protocols, such as those developed as part of the SCA IPR Toolkit. Such strategy will allow the organisation to accrue knowledge from the accumulated clearance experience. It is necessary to properly document the clearance process so that there are records of the material cleared. Ideally, metadata from the rights' documentation should be in a standard form so that other institutions or projects can make use of them.

For small and medium size organisations it is necessary to port ready-made clearance and risk-management procedures and customise them to their personnel and technology requirements. Another solution would be to establish a clearance service for a specific sector (e.g. museums) at national level and thus reduce the costs for individual organisations.

### 4.2.3 Example

The star-shaped model may be applicable even in cases where the organisation collecting the content and the permissions keeps transforming. This is the case of the VoB, where the organisation performing the collection has changed several times due to transformations in the project (see diagram II).

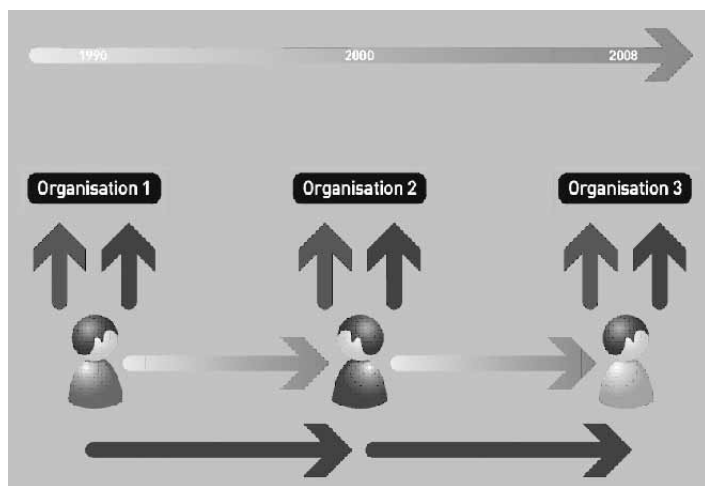


Diagram II

In this case, the continuity of the VoB project has been preserved by ensuring that a single point was responsible for the collection of content and permissions that the star-shaped model provides. This point of collection functions *de facto* as a rights repository and constitutes a solution for ensuring the permissions and content have been collected and the project may continue to exist (see diagram III).

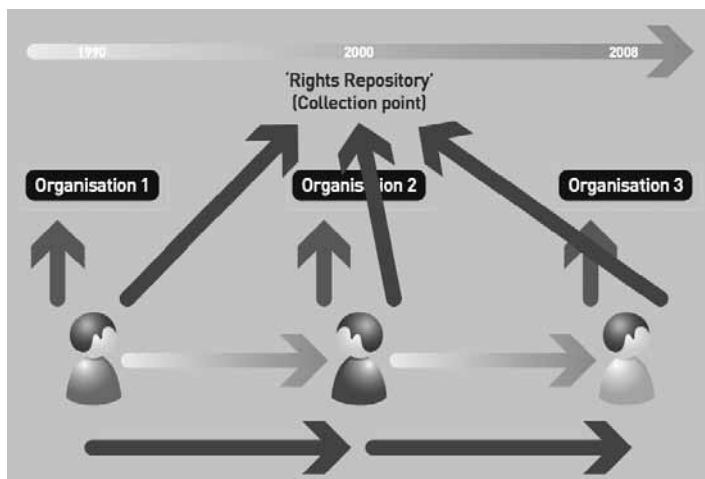


Diagram III

#### 4.2.4 Dissemination

##### Digitisation projects

- Document and standardise clearance processes
- Put a risk assessment and management scheme in place
- Standardise metadata to facilitate communication between different institutions
- Establish a clearance service per sector (e.g. Museums) or region in order to achieve economies of scale.

The dissemination of content may also fit under the star-shaped model. In such cases, both distribution and licensing of content is managed by a single central organisation. In this case, there are three broad scenarios of content and licence distribution under the star-shaped model:

- Public internet distribution
- Walled garden distribution, i.e. restricted distribution
- Hybrid public/walled garden distribution

##### *4.2.4.1 Dissemination over the public internet*

When content is made available over the internet the following are most common characteristics of its dissemination (see diagram IV):

- There is always some form of licence specifying the permissible uses. The End-User Licence Agreements (EULAs) are custom-made licences that reflect the policy and strategy of the specific organisation
- The EULAs allow only private and non-commercial or educational uses. No super-distribution, i.e. further dissemination by the user or publishing on their private website is permitted. Repurposing is usually prohibited as well
- Quality of the digital surrogates is normally low. For instance, low resolution images or videos, low bit-rate sound recordings.
- In cases of audio or video, the content is only made available for streaming, not downloading.
- No Technical Protection Measures (TPM) are used for still images or audio (Akester 2006). However, some of the audiovisual content is protected with TPM and downloading may be allowed only for a limited amount of time (eg BBC iPlayer)
- As a result, the content, both technically and legally, cannot to be re-purposed either by end-users or other public-sector organisations

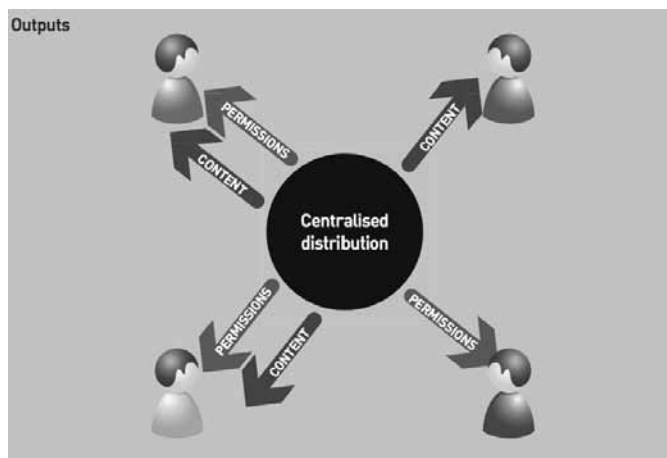


Diagram IV

#### 4.2.4.2 Walled garden distribution

When content is made available over a controlled/secure network, the following are the most common characteristics of its dissemination (see Diagram V):

- Dissemination of content over a secured environment is expressed in the related EULAs and the technologies of distribution. The EULAs are custom-made licences that reflect the funding conditions of the specific digitisation programme (eg the BL SA I was only made available to FE/HE students) or the charter of the digitising organisation (eg BBC content is normally made available only within the UK). The technology normally allows access to the content either through a specific gateway or on the basis of the IP address. For example, in the case of the BL ASR I project, digital audio recordings are made available only to UK HE/FE students and members of staff through the Shibboleth service; the BBC audiovisual content is only made available to users having a UK Internet Protocol address.
- Rights awarded to the users are normally greater than those found over the public internet. They normally include rights of reuse within the specific network. Such is the case of the BL SA II project, where the content is made available for reuse only within the secure network. Such an approach may be problematic as it creates pools of content that because of the licensing terms may not be legally interoperable with content that is reusable under a standard public licence, such as the Creative Commons licences.
- No technical protection measures are used on the actual content but access is allowed only to authorised users over secure networks.

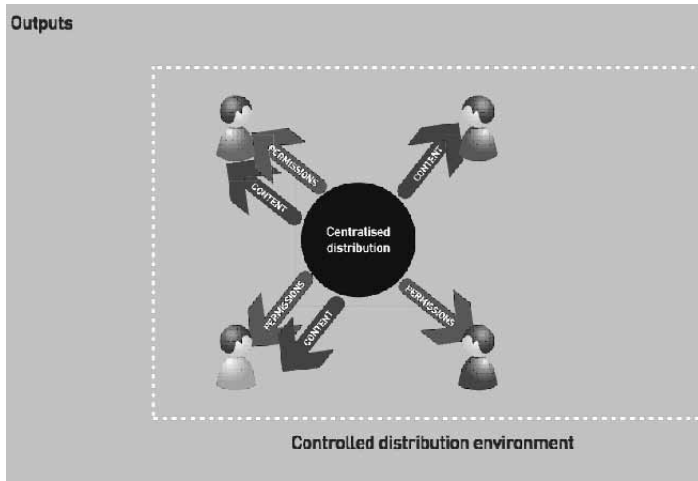


Diagram V

#### 4.2.4.3 Hybrid public internet/walled garden distribution

This is the case when content is made available by the same central point both to the public internet and over a secure network (see Diagram VI). The case applicable in this model is the BL ASR II project. In such a scenario:

- Different sets of content are distributed over public and secure networks, with premium or full content being provided over the latter.
- Different sets of rights awarded to the two types of users (public/within the walled garden). In the case that reuse rights are granted to users within the walled garden, the 'licence dilemma' appears.
- If a standard public licence allowing reuse is used (eg the Creative Commons licences), then the content may be legally and freely disseminated and reused on the public internet.
- If a custom-made licence allowing reusability is employed, then it will be very complex legally (and subsequently very expensive) to combine the walled garden content with free internet content. The creation of content islands may be desirable in the short term but may cause substantial clearance problems or may even make the recombination of the content unusable in the long run.



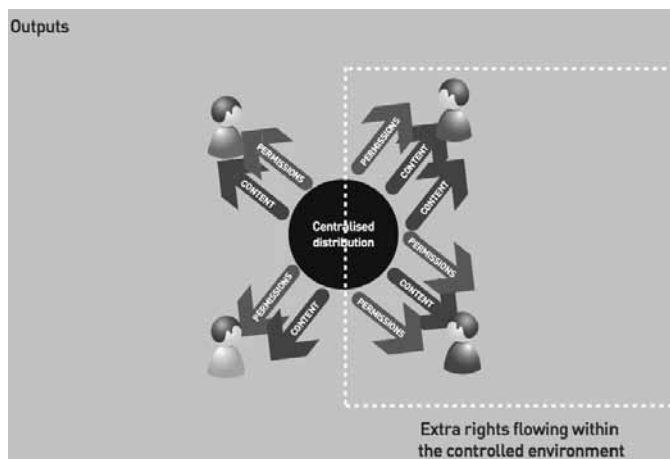


Diagram VI

### 4.3 The 'Snow-Flake' model

In the snow-flake model (diagram VII) the clearance of rights (obtaining permissions) and acquisition of content is organised in clusters: rights are cleared and content is aggregated first locally, then in clusters of local units and finally in a central hub. This type of collection appears in the NLH project and in some sense in the BlueGreece projects. It is a model that allows the reduction of clearance costs for the central organisation: the costs of clearance are primarily covered by the local organisations or at the cluster level. The central organisation oversees and manages the whole process but is not involved in any clearance itself.

Standardised risk management and clearance procedures are quintessential for the success of this model. The central organisation needs to have in place such procedures in order to ensure that the risk of copyright infringements is mitigated.

The snow-flake model is particularly popular in projects that:

- Are geographically dispersed
- Have multiple units
- Deal with more than one type of rights (eg copyright, personal data, protection of minors etc) that can be acquired and managed locally

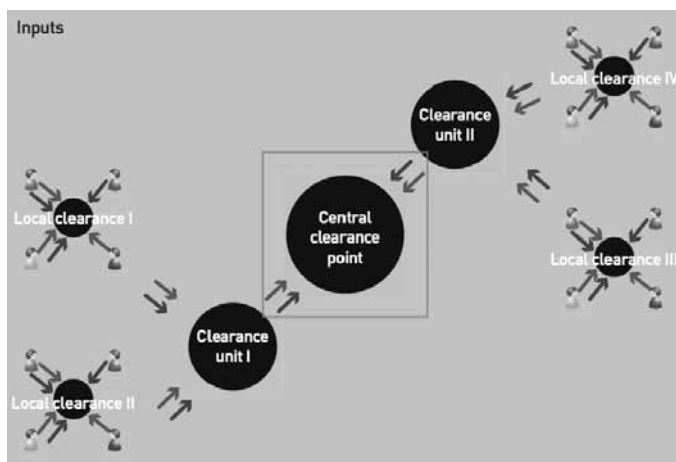


Diagram VII

#### 4.4 The 'Clean-Hands' model

This is the model where the flows of rights and content follow entirely different paths. The content is normally collected and may be downloaded from a single point, whereas the licences flow directly between the users. The central organisation does not deal with copyright at all and that is why we use the metaphor of clean hands to describe the model (see diagram VIII).

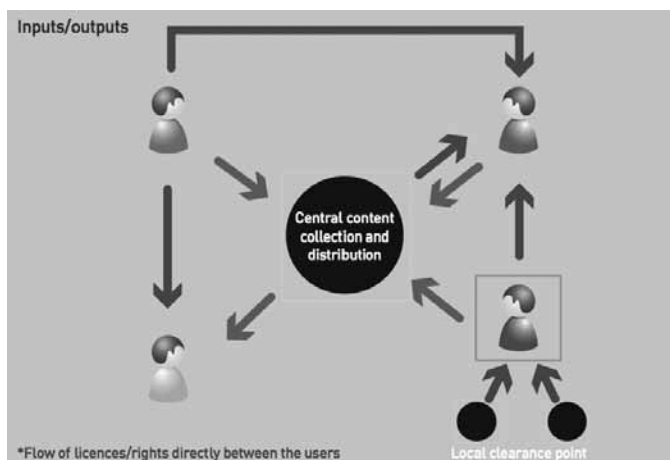


Diagram VIII

The key characteristics of the clean hands model are as follows:

- The clean hands model is not necessarily concerned with the aggregation of content or licences but rather with facilitating the respective flows (of content and licences between the users). The aggregation of content could take place in a centralised fashion and hosted by the central organisation (e.g. in the case of the BlueGreece, Creative Archive and NLH LOR projects), or to be directly managed by the participants of the system (e.g. CenturyShare project). The central organisation is not at all concerned with acquiring any licences over the content. In this model the central organisation only ensures that the end-users have the necessary permissions supplied by the rights owners
- The clearance of the content is pushed at the ends of the network or on the contributors of the content. These may be either individuals, legal persons or other projects. They are responsible not only for the copyright clearance but also for obtaining any other required permission such as Prior Informed Consent or personal data clearances
- The main risk management approach followed by the central organisation relies on their lack of direct involvement in obtaining any permissions for themselves and clearly stating in the service registration agreement that the end-user is responsible for the clearance of rights. Additional necessary measures include the provision of proper disclaimer clauses and clear notice and take-down procedures

#### 4.4.1 Impact

This particular model can result in the possibility of the 'licence pollution' phenomenon. Specifically, in a reuse scenario the copyright licences used have to be compatible with each other, otherwise they will lead to derivative works infringing the copyright of the content on which they are based. For example, all Creative Commons licences are not compatible with each other and if they are used in a service (eg in the NLH LOR project) it is necessary that some minimum care is taken to inform the users accordingly. This may be done by ensuring that in the case of uploading a derivative work, the user is obliged to name the content sources and their respective licence. The system then should automatically inform the user about the compatibility of the source licences

- In any reuse scenario, the rights information should refer to the work, not the creator (see diagram IX). Hence, it is necessary to have metadata attached to each work making explicit:
  - Which works it is based on
  - In which works it has been used

- Overall, it is advisable to use standard licences and metadata so that linking with other organisations and projects is possible
- The more rights are offered to the licensee, the more the need for:
  - Attribution
  - Provenance
  - Quality assurance
  - Adherence to data protection rules, processes for protecting minors and Prior Informed Consent rules

#### **4.4.2 Examples**

The clean-hands model is adopted in the following cases:

The central organisation is interested only in aggregating content from various other organisations or projects that provide content under a variety of licences. In this case, the central organisation may not even host the actual content: it may only provide the links to the content and perform the functions of aggregation and curation. The value, in this case, derives from increasing visibility and associating content with other related content. Therefore any metadata created are normally owned by the central organisation. This is the case of the CenturyShare project

The central organisation is interested in the reuse of content provided either by end-users, other projects or organisations. The value comes from the reuse and incremental improvement of content. These are the cases of the Creative Archive and BlueGreece projects. The central organisation hosts only user-generated content that freely flows on the internet. Value derives again from building on existing material and collective development. By pushing the rights clearance at the ends of the network the organisation decreases clearance costs and mitigates risks. It is not responsible for managing the complex ownership questions that are likely to appear. In this case standardised licences, such as the Creative Commons licences, are used. The most relevant related projects are the NLH LOR project.

#### **4.4.3 Value**

The main sources of value in the clean hands model are:

- The cultivation of communities
- The production of metadata
- The linking of relevant content
- Reduction of redundancies
- Incremental innovation

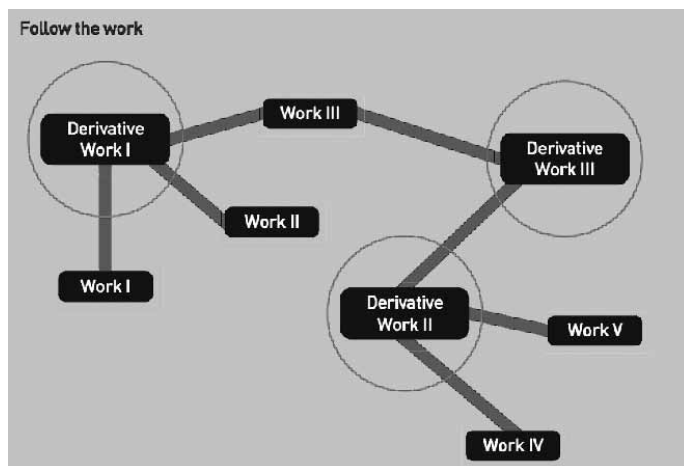


Diagram IX

## 4.5 Conclusion

Irrespective of which model IPR model is to be followed, a suitable copyright management framework needs to be implemented to ensure that basic procedures and decision-making rules can be widely adopted. This will ensure that staff and users understand the nature of the permissions that are being granted regarding access and use of content.

## References

- Aigrain, P. (1997). "Attention, Media, Value and Economics." *First Monday* 2(9).
- Akester, P. A. R. (2006). "Digital Rights Management in the 21st Century." *European Intellectual Property Review* 28(3): 159-168.
- Bansal, L., P. Keller, et al. (2006). *In the Shade of the Commons: Toward a Culture of Open Networks*. New Delhi, Waag Society, Amsterdam, The Netherlands.
- Barlow, J. P. (1994). *The Economy of Ideas*. *Wired*. 2.
- Benkler, Y. (1999). "Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain." *New York Law Review* 74(354).
- Bernstein, S. (2008). *Where Do We Go From Here? Continuing with Web 2.0 at the Brooklyn Museum*. *Museums and the Web*, Toronto, Archives & Museum Informatics.
- Black, J. (2000). "Proceduralising Regulation: Part I." *Oxford Journal of Legal Studies* 20(4): 597-614.

Black, J. (2001). "Proceduralising Regulation: Part II." *Oxford Journal of Legal Studies* 21(1): 33-58.

Boyle, J. (1992). "A Theory of Law and Information: Copyright, Spleens, Black-mail and Insider Trading." *California Law Review* 80: 1413.

Boyle, J. (1996). *Shamans, Software and Spleens: Law and the Construction of the Information Society*. Cambridge, Mass.; London, Harvard University Press.

Boyle, J. (2008). *The public domain: enclosing the commons of the mind*. New Haven, Conn.; London, Yale University Press.

Brito, J. and B. Dooling (2005). "An Orphan Works Affirmative Defense to Copyright Infringement Actions." *Michigan Telecommunications and Technology Law Review* 12(Fall): 75-113.

Ciborra, C. (2004). *Digital technologies and the duality of risk*. London, ESRC Centre for Analysis of Risk and Regulation.

Creative Archive Licence Group. (2006). "BBC Creative Archive Pilot has Ended." Creative Archive Retrieved 31.10.07, 2007, from [http://creativearchive.bbc.co.uk/news/archives/2006/09/hurry\\_while\\_sto.html](http://creativearchive.bbc.co.uk/news/archives/2006/09/hurry_while_sto.html).

Dietz, S. (1998). *Curating (on) the Web. Museums and the Web: An International Conference*. Toronto, Ontario, Canada, Archives & Museum Informatics.

Dyson, E. (1995). *Intellectual Value: A Radical New Way of Looking at Compensation for Owners and Creators in the Net-based Economy*. *Wired*. 3: 11.

Elkin-Koren, N. (1997). "Copyright Policy and the Limits of Freedom of Contract." *Berkeley Technology Law Journal* 12(1): 93.

Elkin-Koren, N. (1998). "Copyrights in Cyberspace -- Rights Without Laws?" *Chicago Law Review* 73: 1115.

Elkin-Koren, N. (2005). "What Contracts Cannot Do: The Limits of Private Ordering In Facilitating a Creative Commons." *Fordham Law Review* 74(November): 375-422.

Elkin-Koren, N. (2006). *Exploring Creative Commons: A Skeptical View of a Worthy Pursuit. The Future of the Public Domain*. B. Hugenholtz and L. Guibault, Kluwer Law International.

Ghosh, R. A. (1998). "Cooking Pot Markets: An Economic Model for the Trade in Free Goods and Services on the Internet." *First Monday* 3(3).

Gordon, W. J. (1989). "An Inquiry into the Merits of Copyright: The Challenges of Consistency, Consent and Encouragement Theory." *Stanford Law Review* 41: 1343.

Huang, O. (2006). "U.S. Copyright Office Orphan Works Inquiry: Finding Homes for the Orphans." *Berkeley Technology Law Journal* 21: 265-288.

Hutter, B. M. (2006). *Business Risk Management Practices: The Influence of State Regulatory Agencies and Non-State Sources*. The Centre for Analysis of Risk and Regulation: Discussion Papers. London, The London School of Economics: 1-29.

Lessig, L. (2006). *Code: version 2.0*; Lawrence Lessig. New York, BasicBooks; [London: Perseus Running, distributor].

Lessig, L. (2007, 01.10.07). "Creative Commons @ 5 Years." The Lessig Letter Retrieved 09.10.07, 2007, from <http://lists.ibiblio.org/pipermail/cc-lessigletter/2007/000022.html>.

Lezaun, J. and L. Soneryd (2006). *Government by Elicitation: Engaging Stakeholders or Listening to the Idiots*. The Centre for Analysis of Risk and Regulation. London The London School of Economics and Political Science: 1-31.

Murray, A. (2007). *The Regulation of Cyberspace: Control in the Online Environment*. New York, Abingdon, Routledge-Cavendish.

Murray, A. and C. Scott (2002). "Controlling the New Media: Hybrid Responses to New Forms of Power." *The Modern Law Review* 65(4): 491-516.

Pasquale, F. (2006). "Toward on Ecology of Intellectual Property: Lessons from Environmental Economics for Valuing Copyright's Commons." *Yale Journal of Law and Technology* 8: 78.

Paulk, M. C. (1995). *The Capability Maturity Model: Guidelines for Improving the Software Process*. Reading, Mass., Addison-Wesley Pub. Co.

Pollock, R., D. Newbery, et al. (2008). *Models of Public Sector Information Provision via Trading Funds*. London, BERR and HM Treasury.

Samis, P. (2008). *Who Has The Responsibility For Saying What We See? Mash-ing up Museum, Artist, and Visitor Voices, On-site and On-line*. Museums and the Web 2008, Toronto, Archives & Museum Informatics.

Schultz, M. F. (2007). *Copynorms: Copyright and Social Norms*. Intellectual property and information wealth: issues and practices in the digital age. P. K. Yu. Westport, Conn.; London, Praeger: 4 v.

Sterling, J. A. L. (2003). *World Copyright Law: Protection of Authors' Works, Performances, Phonograms, Films, Video, Broadcasts and Published Editions in National, International and Regional Law: with a Glossary of Legal and Technical*

Terms, and a Reference List of Copyright and Related Rights Laws throughout the World. London, Sweet & Maxwell.

Taylor-Gooby, P. and J. Zinn (2006). *Risk in Social Science*. Oxford, Oxford University Press.

Tsiavos, P. (2006). "Re-inventing Protection: Autonomy, the Commons and the Untold Copyright Saga." *First Monday* (Special Issue: FM10 Openness: Code, Science and Content).

Watt, R. (2000). *Copyright and Economic Theory: Friends or Foes?* Northampton, MA, E. Elgar.

Wu, T. (2003). "When Code Isn't Law." *Virginia Law Review* 89 (June): 679-751.

Young, A. (2005). *Judging the Image: Art, Value, Law*. London, Routledge.



# Transposing the Data Retention Directive in Greece: lessons from Karlsruhe

---

Anna Tsiftoglou & Spyridon Flogaitis

---

## I. Introduction

In the Academy-Award winning film *Das Leben der Anderen* (The Lives of Others), a 1984 East Berlin memoir, a Secret Police agent is assigned the task of listening to the private life of an artist couple. As his task requires, he drafts detailed reports of all their home conversations and actions, seeking evidence of suspicious behavior towards the existing Regime. Accustomed to conducting surveillance, the Stasi Agent gradually becomes absorbed by his subjects' intimate lives.

If art depicts reality or is, at least, inspired by reality, then films like the latter should trigger us to think – if such practices were conducted under oppressive regimes, could we legitimize them within a democratic state? And if so, under what circumstances?

The German Constitutional Court attempted to give answers to such hard questions. Applying strict scrutiny on a federal law implementing the contested Directive 2006/24/EC ('the Data Retention Directive'), it nullified it on proportionality grounds (Federal Constitutional Court of Germany, 2010). The case serves as an example to -among others- the Greek legislator, who only recently implemented the Data Retention Directive, as well as to the Greek courts, which may encounter possibly similar challenges. Moreover, there are lessons to be learned from the Karlsruhe Court, both from a constitutional law perspective and from its stance towards EU regulation & control of public safety measures. One thing is certain: there are tough times ahead.

## II. Transposing the DRD: What Karlsruhe said

On March 2<sup>nd</sup> 2010, the *Bundesverfassungsgericht* (BVerfG) overturned a German federal law implementing the Data Retention Directive (BBC News, 2010; Privacy International, 2010). The 2008 federal law [*Gesetz zur Neuregelung der Telekommunikationsüberwachung- GNTR*] amended several provisions of the German Criminal Procedure Code [*Strafprozeßordnung- StPO*, art.100g par.1§1] and of the German Telecommunications Act [*Telekommunikationsgesetz- TKG*, art.113a, b].

The amended provisions called for a 6-month preventive retention of all traffic and location communications data (not content), to be retained mandatorily by communications service providers [113a TKG] for the broadly defined purposes of crime prosecution, combating serious threats to public safety or performance of intelligence tasks [113b TKG]. Moreover, access to such data for crime prosecution purposes would be permitted under a vague provision covering retention of traffic data in general, thus also for commercial aims [100g (1) StPo], without further guarantees.

While the BVerfG did not question the constitutionality of the Directive *per se*, nor accepted the request for a preliminary ruling [267 TFEU] to the ECJ on this matter, it found data retention to be permissible in principle as a security measure. The BVerfG thereafter performed strict scrutiny on the national provisions implementing it.

### ***Ila. Applying the Privacy Test***

Since the above telecommunications surveillance measures constituted an interference to the confidentiality of communications, the BVerfG had to judge them under the light of Article 10 of the German Constitution (*Grundgesetz* –GG), protecting the ‘Privacy of Correspondence, Posts and Telecommunications’. Article 10GG protects all kinds of communication, electronic or otherwise, and extends *both to the actual content and its circumstances*, thus *also to traffic and location data* [BVerfG, §§189-190]. In addition, the provisions would be judged under the light of the fundamental right to informational self-determination (*‘informationelle selbstbestimmung’*), jurisprudentially created by the very same court in the notable 1983 ‘Census Case’ (Skouris, 1984, pp.692-694; Goold, 2007, pp.65-67; De Simone, 2010, pp.292-295). The latter right is a ‘precursor’ to the newer ‘right to data protection’, protected under the EU Charter of Fundamental Rights (art.8), as well as an aspect of *privacy* under the European Convention on Human Rights (art.8) (Simitis, 2010, p. 1992-93, 1997-98).

To check the constitutionality of the amended national provisions, the Karlsruhe Court applied a Privacy Test similar to the one employed by the European Court of Human Rights (‘the Strasbourg Court’) (De Vries et al., 2011, pp. 6-8). The Strasbourg Court has developed this test when performing checks on restrictions to privacy under article 8§2 ECHR (Tsiftoglou, 2011, pp.95-96). The privacy test followed by the BVerfG follows the Strasbourg Court three-level formulation (Tzanou, 2011, pp.281-283), though placing more emphasis on the final level (proportionality check), as follows:

- A. Legality check [quality of the legal basis]: the interference must be founded on a law that is accessible and foreseeable, a standard satisfied by the above provisions
- B. Legitimacy check [legitimate aim]: the interference must be justified by a legitimate aim, here viewed as “effective criminal prosecution” and prevention of dangers”
- C. Proportionality check: a broader check of the nature of the interference comprising of checks on: a. data security standards, b. purpose limitation, c. transparency and d. legal protection (judicial control)/ sanctions

The final (proportionality) check is thus the most crucial one for the Karlsruhe court. Whereas the former two levels (legality & legitimacy) could relatively easily be satisfied, the last level requires additional guarantees to counter-balance the intensity of the interference to the fundamental right to telecommunications privacy.

The intensity of the interference is boldly acknowledged by the BVerfG, which talks about the danger of a ‘diffuse threat’ of being under constant surveillance [§§241-242] that may ultimately have a chilling effect on the exercise of other rights, such as freedom of speech. Solove, an American privacy expert, stresses that “Even surveillance of legal activities can inhibit people from engaging in them [...] Chilling effects harm society because, among other things, they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity” (Solove, 2007, 765). This ‘side’ or ill effect of massive surveillance had been emphatically asserted by the BVerfG in the Census Case (DeSimone, 2010, pp.294-5):

“Whoever is unsure if their dissenting behavior may be recorded at any time and, as information, permanently saved, will try to avoid attracting attention through such behavior. This would impair not only the personal development chances of individuals, but also the public good, as self-determination is a prerequisite for a free democratic polity based on its citizens’ capacities of civic action and collaboration”.

Judges Schluckebier and Eichberger, in their dissent, expressed the view that retention of traffic and location data cannot be considered an ‘intense’ interference or at least comparable to other forms of surveillance. This, they argued, was due to the fact that retention does not extend to content, the fact that all retained data are dispersed within servers of private parties and the fact that a judicial order is required for access to data.

However, the majority of the BVerfG recognizes that this kind of massive surveillance without occasion constitutes ‘an especially heavy rights burden...with a dispersion, as yet unseen in our legal system to date’ [§§210-212]. Even if retention does not cover the actual content of communications, the retained data may be

used to create 'meaningful personality profiles of virtually all citizens and track their movements'. Thus processing of such vast amounts of communications data may help construct social profiles for every possible user, a scenario that the Karlsruhe court finds truly disturbing.

Profiling techniques are becoming, though, an increasingly useful tool for law enforcement agencies within Europe. The police utilize them to target 'not just criminal, but also more generally deviant behavior' (Brown & Korff, 2009, 5, 9). The emphasis now shifts from defendants to abstract suspects (Paraskevopoulos, 2004, 50, 58).

Nevertheless, the BVerfG finds that, despite its intense character, data retention is not unconstitutional in principal, given its features [§§205]. The disperse nature of retention by private actors (not the State) as well as its limited duration (6 months – minimum set by the Directive-art.6) seem, in the Court's view, to ease the intensity of the encroachment to the right to communications privacy (10GG). Overall, the exceptional character of this precautionary measure to serve important public interests such as the combating of organized crime contributes to its judicial acceptance, provided that additional conditions, set by the Court, are fully satisfied.

To pass the proportionality check, specific criteria have to be met. These preset conditions (purpose limitation, data security standards, transparency and effective legal protection) relate principally to the quality of the law (Breyer, 2005, pp. 366-373; Pinakidis, 2007, pp. 422-426), which the Strasbourg Court places in the primary (legality) check (De Vries et al, 2011, p. 6). The presence of procedural safeguards had been underlined immediately following the voting of the Data Retention Directive, in view of a uniform implementation of data protection standards throughout Europe (Article 29 Working Party, 2006). The *ratio* is that the national legislator should offer serious counter-balances for the intensity of this security measure.

### **i. Purpose Limitation**

Given the nature of the intrusion, data retention may only be permitted for limited purposes. Thus, the common legislator ought to minimize the scope of communications data use by enlisting specific data uses. As such, the prescribed purposes of data retention, as listed under the provisions of StPO &TKG, must be substantively limited.

(1) "Criminal Prosecution" should be clarified by a list of serious crimes, possibly specified by type (i.e. felonies only) for which concrete suspicion & proof is necessary;

Article 100g (1) StPO, to which §113b TKG refers, does not satisfy these conditions. Section 100g (1) (1) StPO allows direct use of communications data if a person “has committed a criminal offence of substantial significance”, a vague term left to multiple interpretations, instead of enlisting a numerous *clausus* of serious crimes only (§228). Section 100g (1) (2) StPO is drafted in an even more generic manner, as it allows for direct use of communications data if a person “has committed a criminal offence by means of telecommunications”. Given the central role of telecommunications nowadays, such a clause permits direct data use for virtually any crime, regardless of its seriousness. Thus the scope of data retention ‘for criminal prosecution’ is magnified to an extent possibly not envisioned by the drafters of the Data Retention Directive Whereas data retrieval is permitted only in limited cases and under a judicial order, the current provisions treat this measure as a norm (§278) even “without the knowledge of the person concerned”, contrary to the general duty of notification (101(4) (6) StPO). Moreover, no judicial control is hereby provided in case of failure of notification (Antonioni, 2008, 25-28; Kaiafa-Gbanti, 2010, 43-45; Tzalavra, 2007, 566-567).

(2) “Prevention of hazards to public safety” must be limited to only serious threats to a person’s high values or to the integrity of the State. The same applies to (3) performance of intelligence tasks” (§231-232). In addition, where certain confidentiality relationships (i.e. emergency phone calls seeking help) apply, data retention should be totally prohibited, given the nature of such communications.

Sections 113b (2) and (3) TKG are also drafted in an unacceptable generic manner and satisfy very broad objectives. TKG leaves great space to future legislative acts (on a Federal or especially State level) to specify this objective, thus opening ground for multiple and extensive uses of communications data, which is greatly disproportionate.

The above restrictions are less stringent regarding indirect use of communications data. That is, in cases where public authorities request only user identifying information- such as info resulting from collected IP addresses- from service providers. The Court does not take any position on whether IP addresses (static or dynamic) should be considered “personal data” (according to article 2 of Directive 95/46/EC) (Fragkouli, 2008, p.204). At any case, this right to information is viewed as a moderate interference to the right to communications privacy; however, it is also subject to conditions, given its impact on the anonymity of Internet communications. Anonymity on the Internet should only be lifted for substantial and serious public interests, which are precisely specified by law. As such, a blanket right to information for the general purpose of “criminal prosecution” (Section 113b TKG) and with no notification of the data subject attached is considered unconstitutional by the Court.

## ii. Data Security Standards

A high degree of data security standards is required (§222). The legislator can assign an independent authority the task of drafting detailed and legally binding provisions to ensure the implementation of such standards in data processing. Moreover, additional measures should be taken to limit the service providers' discretion in applying data security standards and subject data processing to effective supervision.

The required high degree of data security standards is hereby *missing*. Article 113a§10 TKG is drafted in a *generic* manner that leaves discretion to the private parties (service providers) to define the appropriate standards themselves. However, such clauses do not guarantee any quality standards neither can be enforceable, since no sanctions are provided to punish serious data security violations.

## iii. Transparency of Processing

All data processing must be transparent. Exceptions should be allowed only in cases where the purpose of data retention would otherwise be frustrated, such as in certain criminal prosecution acts or while carrying out intelligence tasks. Even in those cases judicial oversight is required, as well as a posteriori notification of the subject (§243).

## iv. Effective Legal Protection

Data subjects must be protected against the secrecy of data processing. Thus judicial control is mandatory, as a form of resistance, to prevent arbitrariness as well as to offer recourse to potential victims of unlawful processing (Paraskevopoulos, 2004, 53, 55). Additionally, effective legal sanctions against rights abuse and liability of service providers for damages caused should be essentially provided by the legislator (§252).

Overall, the present structure of the above provisions lacks the mandatory standards of purpose limitation, high data security and transparency guarantees as well effective judicial control and sanctions. As such, these clauses are considered disproportionate and, thus, unconstitutional contrary to 10GG. Therefore, the Court declares them void.

Interestingly, the contested provisions were deemed contrary only to the right to communications privacy (10GG) and not to the right to self-determination. The BVerfG however extended the protective shield of 10GG to traffic and location data (circumstances and not mere content of communication) and to any further data processing conducted following their retention and information gathering (§§ 188-190).

Judge Schluckebier, in his dissent (§§ 310-336), accused the Majority for judicial activism and of dictating the legislature how to balance competing interests. Given the changing nature of organized crime, the state must conform to the challenges posed by technology and develop measures such as data retention that effectively serve the duty to protect its citizens. By restricting access and use to retained data, the majority basically restricts the legislator's freedom and power to regulate and thus surpasses its duty of judicial self-restraint. Surprisingly, Judge Schluckebier noted that, while the Majority acknowledged the challenges posed by technology in order to assess the intensity of interference, it did not reach any similar conclusions regarding the State's positive obligation to protect citizens against modern risks (Brown & Korff, 2009, 9).

### ***Iib. The Role of Telecommunications Service Providers***

An interesting aspect of this case is the role assigned to telecommunications service providers. The BVerfG considers them as 'guarantors' of the retained data, to which state authorities have access, directly or indirectly, only in limited occasions (§214).

This approach, however, rests on a fallacy, since nowadays several private parties tend to be much more powerful and effective than the State. We actually experience a form of "distributed surveillance", an evolving public-private network where several private enterprises act as Government agents (Mitrou, 2010, 140-141). "The Government no longer sticks to the traditional direct collection of data. It turns instead to private entities. In doing so, the State not only acknowledges that the majority of data is stored in the private sector, but also establishes a processing model systematically combining information gathered in both public and private sectors" (Simitis, 2010, 2003). Indeed, prominent American web-services companies such as Google and Facebook control today vast amounts of personal data, while their relationship with the US Government may not be as transparent as it seems (De Vries et al, 2011, p.9; Info Wars, 2011).

The European legislator entrusts private parties with a duty of storage for security purposes, additional to storage for their obvious commercial purposes, which imposes a considerable financial burden on them. Nevertheless, it is uncertain who is paying this price. Service providers in Germany are obliged to bear this cost on their own. Such industry-wide costs ranged between €130 million in France in 2006 (Pateraki, 2011, 324) to €150 million in the UK alone in 2008 (DeSimone, 2010, 310). Even worse, the lack of harmonization in this respect has serious financial impacts on competition in the EU telecoms market (Iglezakis, 2009, 1285; Sotiropoulos & Talidou, 2006, 185).

Rejecting allegations about the unconstitutionality (12GG- occupational freedom together with 14GG- private property) of such a burden and demands for compensation, the BVerfG confirmed that the cost associated to the duty of storage (113a TKG) does not exceed the obligations of service providers, as long as it is proportional. “Entrusting private entities with public duties is not, in itself, constitutionally problematic, nor does it require public reimbursement for private expenses” (§301). The BVerfG does not seem to take into account protection of property under the First Protocol to the ECHR [article 1(2)] either. The latter would definitely call for adequate compensation for such state-imposed obligations to service providers (Breyer, 2005, 374-375).

In the Court’s view, the burden of cost should be assumed by the market, and be shifted eventually to consumers. With this ‘twisted’ frame of logic the citizens will be obliged to pay for their own surveillance! (Kaiafa-Gbanti, 2010, p.43).

### ***IIc. Karlsruhe v. Luxembourg: Tough Times Ahead!***

Another interesting aspect of the case is how the Karlsruhe court tries to ‘avoid dialogues’ (Papadopoulou, 2009, 382-4) with the European Court of Justice (ECJ)

The core issue brought forward to Karlsruhe was the constitutionality of the Directive itself, rather than the various national laws implementing it. The German court however lacked jurisdiction to originally interpret EU law. Nevertheless, it declined to refer the matter to Luxembourg, by relying on a former ECJ decision to illustrate how core criminal affairs still rest on the imperium of national legislators and courts.

In February 2009, the Luxembourg Court, in C-301/06 (*Ireland v. Parliament and Council*) rejected Irish claims on the wrongful adoption of the Data Retention Directive. Instead, it confirmed that former article 95 EC (now 114 TFEU) constituted the appropriate legal basis for the Directive as a former First Pillar measure, since the Directive’s prime objective was to harmonize internal affairs within the EU telecommunications market (Loideain, 2011, p.260; Igglezakis, 2009, 1281-1286). By rejecting Irish allegations about *ultra vires* adoption of the Directive, the Luxembourg Court erred in its reasoning to decline that the directive’s objectives were properly classified under the former EU Third Pillar. Characteristic in this respect is article 9 of the Preamble to the Directive which states ‘Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organized crime and terrorism...’. Moreover, the Luxembourg Court avoided exercising scrutiny on this Directive for compliance of to the



ECHR standards (Breyer, 2005, 366; Pinakidis, 2007, 422-437) as data retention was considered merely as a First Pillar measure.

The adoption of data retention as an 'internal market affairs' issue by co-decision of the EU Parliament and the Council was not random. A product of political compromises between central EU institutional actors (the Council, the Commission, the Parliament and data protection bodies) it strengthened the Parliament's powers on the matter, which would have been impossible if a different legislative instrument, such as a framework decision, was chosen (DeSimone, 2010, 301-303; Antoniou, 2008, 14-17; Sotiropoulos & Talidou, 2006, 185-193). Thus the debate over the legal basis of this measure 'was not about rights but about the nature of EU democracy' (Bignami, 2007, 244, 238-251).

While the European Union was primarily conceived as an economic union, the emphasis following terrorist attacks in New York, Madrid and London seems to have shifted towards the creation of a political union, through the promotion of enhanced law enforcement cooperation policies. As such, 'The European Union is proving to be the nation-state in reverse chronology. The functions that the nation-state developed first – protection from physical violence – the European Union is acquiring last. Those functions that the nation-state acquired last – administrative regulation of complex markets – the European Union took on first' (Bignami, 2007, 233, 253).

As confirmed by the ECJ and highlighted by the Karlsruhe court (§§80-83), data retention and storage by telecommunications service providers are regulated by the Directive (articles 1-3), while access to and use of the retained data are left to Member State discretion (articles 1, 4, 6, 12) (Gerontas, 2007, 49). The principle of Subsidiarity, a procedural rule managing shared competences (Rantos, 1995, 32, 34-6), is hereby applied flexibly: *data retention and storage* are regulated by EU law whereas the issues of *access to and use of data* are regulated by national law. This sharp distinction also corresponds to a set of different actors: access and use are treated as law enforcement policies and are thus decided by national police authorities, who act with a great margin of appreciation. The Karlsruhe court clearly uses this distinction to its own advantage: since the core issues of the constitutional complaints touch upon *access and use*, then referral to Luxembourg is deemed unnecessary (De Vries et al, 2011, 12-13).

The tension between the 'integration-oriented' approach of the Luxembourg Court and the 'protection of sovereignty' approach (Kokott, 2010, 100-101) is hereby evident. The Karlsruhe court, by avoiding dialogues with Luxembourg, is seeking to preserve its status as 'the ultimate interpreter of constitutional legitimacy' (Papadopoulou, 2009, 148-150). A statement is declaratory: "The fact that the exercise of civil freedoms cannot be totally recorded belongs to the German

Constitutional identity, which Germany must seek to preserve in European and international contexts" (§218). The respect of the German constitutional identity is thus presented by the Karlsruhe Court as an ultimate limit to control human rights degradations imposed by the European legislator on security grounds (Tsatsos, 2005, 24; Papadopoulou, 2009, 380-381). In an age of rapidly evolving European integration, the BVerfG should serve as an example for other Constitutional Courts and restate its relationship with Luxembourg by regaining 'the lost balance'. As Advocate General Kokott suggests, 'The German Constitution has no monopoly on the ideal protection of democracy, the rule of law and fundamental rights. (...) The solution must lie in recalling the international and open spirit in which the Basic Law was drafted and adopted in 1949' (Kokott, 2010, 102).

### III. Transposing the DRD in Greece: Law 3917/2011

The Greek legislator transposed the Data Retention Directive in February 2011 with Law 3917/2011 (Government Gazette No. 22A/21.02.2011). This transposition was completed with considerable delay followed by a bitter ECJ ruling imposing a fine for failure of timely transposition (C-211/09, *Commission v. Greece*).

Nevertheless, the Greek transposition should be judged overall positively. By treating traffic and location data as elements of intimate communication, the Greek legislator subjects them to the enhanced guarantees of Article 19 of the Greek Constitution (an analog to 10GG) that protects the privacy of communications. Thus, traffic and location data can be retained only for limited purposes, as stated under the provisions of Executive Law 2225/1994 governing the waiving of confidentiality. As such, data retention is allowed only for an exclusive list of crimes (article 1), while access to the retained data is permitted only to the competent authorities and according to the conditions and procedures described in the Executive Law (article 4).

Furthermore, the Greek legislator provides additional guarantees such as limited location (Greece) and duration (12 months) of retention, the automatic destruction of retained data by service providers upon the end of provided duration as well as various data security principles (articles 6, 7). The latter shall be specified by a complete data security plan drafted by service providers. Lastly, Law 3917/2011 provides strict criminal and administrative sanctions in case of data security breach (articles 11, 12) and civil liability for possible damages caused (article 13).

Despite the above full spectrum of *essential* procedural guarantees (Gerontas, 2007, 66-67; Antoniou, 2008, 31), the Greek legislator fails to provide the most crucial one: effective control. By allocating shared competences (articles 7§2, 9 and 12§2) and overlapping responsibilities (articles 7§2 and 8§2, 9) to two in-

dependent administrative authorities (DPA – the Data Protection Authority- and ADAE –the Hellenic Authority for Communication Security and Privacy) the Greek legislator unsuccessfully attempts to balance competing elements: effectiveness of data protection control with ‘institutional verbosity’.

It is thus puzzling why one of the two rapporteurs argued that a possible merger of the two authorities would constitute a threat to the right to data protection and the right to telecommunications privacy (Pavlopoulos, 2011, 131) Since the Greek Constitution (articles 9A and 19) does not seem to prohibit such a merger, and given the central role afforded to independent administrative authorities as ‘counterbalances’ within its system (Flogaitis, 2001), this might have been a good idea both logistics-wise and in terms of administrative effectiveness.

#### **IV. Lessons from Karlsruhe: What Lies Ahead?**

Overall, we are eager to see the evolution of the data retention matter on two levels. First, on a regulatory level. EU Home Affairs Commissioner Malmström has announced a possible amendment of the Data Retention Directive, following the publication of its long-awaited evaluation in 2011 (Hustinx, 2010, 5). Second, on a judicial level. Since 2008, several national supreme courts in at least six Member-States (Bulgaria, Romania, Germany, Ireland, Cyprus and, most recently, the Czech Republic) have declared national laws implementing the Data Retention Directive unconstitutional. Most importantly, the constitutionality of the Directive is currently pending before the ECJ, after a referral again thanks to Irish initiative (Loideain, 2011, p.266).

BVerfG President Papier called the data retention ruling as ‘One of the most important’ [and also the very last] of his tenure (DeSimone, 2010). Indeed, this German ruling will be a reference point to other courts and legislators around Europe in years to come.

If data collection is deemed essential for the State’s very self- existence (Geron-tas, 2007, 55-56) and even if it is promoted as a ‘temporary measure’ in the fight against terrorism (Weinreb, 2007, 483, 486) it must still be subject to guarantees. It should be allowed for very specific uses, to prescribed authorities, for limited times and under judicial control. A high level of data security must be ensured, and should not be left on the discretion of private parties. Effective sanctions should punish violators. Independent administrative authorities could play a crucial role in these practices, both by imposing regulatory standards and by intervening when needed as watch-dogs (Papakonstantinou, 2006, 446; Tsiliotis, 2006, 541-542; Tsiftoglou, 2011, 98-99)

Moreover, the BVerfG highlighted the importance of proportionality as a measure of justice. Counter-terrorist measures have to be judged from different angles, and both good regulators and hard-working judges have to equally contribute in this respect.

Lastly, the biggest lesson from Karlsruhe should be that self-regulation does not suffice. The legislator, European and national, should impose, as clearly pronounced by the German justices, mandatory privacy standards and rules to all private actors (Simitis, 2010, 2004). In the words of former BVerfG Vice-President Hassemer, 'The State is no longer the Leviathan (...) Instead, the State has become, so to speak, civilized. Citizens no longer see the State as a cause of risks, but see risks as originating outside of the state, from third parties. And they see the state as a possible partner, a potential ally in overcoming these risks' (Hassemer, 2004, 605).

In an era of social networks and of 'diminishing privacy' the State must persistently prove to be the biggest alliance for all citizens.

## References

Antoniou Th. (2008), Telecommunications Privacy on Trial: Directive 2006/24/EC under Transposition, *Applications of Public Law*, 1 [in Greek], 13-31

Article 29 Working Party (2006), [WP 119] Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending directive 2002/58/EC, online at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp119\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp119_en.pdf) - last accessed 15.03.2011

BBC News (2010, March 2), German Court Orders Stored Telecoms Data Deletion, online at <http://news.bbc.co.uk/go/pr/fr/-/2/hi/europe/8545772.stm> - accessed 3.3.2010

Bignami F. (2007), Privacy and Law Enforcement in the European Union: The Data Retention Directive, *Chicago Journal of International Law*, 8, 233-255

Breyer P. (2005), Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, *European Law Journal*, 11:3, 365-375

Brown I. and Korff D. (2009), Terrorism and the Proportionality of Internet Surveillance, *European Journal of Criminology*, 6:2, 119-134

DeSimone Ch. (2010), Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive, *German Law Journal*, 11:3, 291-317

DeVries K., Bellanova R., De Hert P. and Gutwirth S. (2011), The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't it?), in Gutwirth S. et al (eds.), *Computers, Privacy and Data Protection: An Element of Choice*, Springer

Federal Constitutional Court of Germany (2010), Press Release No. 11/2010 concerning the Judgment of 2 March 2010 - 1 BvR 256/08, 1BvR 263/08, 1 BvR 586/08, online at <http://www.bundesverfassungsgericht.de/en/press/bvg10-011en.html> -accessed 3.3.2010

Flogaitis Sp. (2001), The Independent Administrative Authorities, *Ta Nea* [in Greek], January 23<sup>rd</sup>, 2001

Fragkouli Ath. (2008), Are IP Addresses Considered Personal Data and Under What Consequences?, *Mass Media & Communication Law Review*, 2 [in Greek], 198-204

Gerontas Ap. (2007), Personal Data Protection – Public Security or Protection of Basic Rights?, *Applications of Public Law*, Special 20<sup>th</sup> Anniversary Issue [in Greek], 31-68

Goold B. (2007), Privacy, Identity and Security in: Goold B. and Lazarus L. (eds.), *Security and Human Rights*, Hart Publishers

Hassemer W. (2004), “The State is No Longer the Leviathan”, Interview of the German Federal Constitutional Court Vice-President, *German Law Journal*, 5:5, 603-607

Hustinx P. (2010), *The Moment of Truth for the Data Retention Directive*, Speech given at the Conference “Taking on the Data Retention Directive, Brussels, December 3<sup>rd</sup> 2010

InfoWars (2011, February 17), *Facebook and Google are CIA Fronts*, online at <http://www.infowars.com/facebook-google-are-cia-fronts>, last accessed 30.03.2011

Iglezakis I. (2009), The Electronic Communications Data Retention after ECJ Decision C-301/06 of 10.02.2009, *Armenopoulos*, 8 [in Greek], 1278-1286

Kaiafa-Gbanti M. (2010), *Surveillance Models in the Security State & Fair Criminal Trial* [in Greek], Nomiki Vivliothiki Publications

Kokott J. (2010), The Basic Law at 60: From 1949 to 2009: The Basic Law and Supranational Integration, *German Law Journal*, 11:1, 99-114

Loideain N. (2011), The EC Data Retention Directive: Legal Implications for Privacy and Data Protection in: Akrivopoulou C., Psygkas A. (eds.), *Personal Data Privacy & Protection in a Surveillance Era: Technologies & Practices*, IGI Global

Mitrou L. (2010), The Impact of Communications Data Retention on Fundamental Rights and Democracy – The Case of the EU Data Retention Directive in: Haggerty D. & Samatas M. (eds.), *Surveillance and Democracy*, Routledge

Papadopoulou L. (2009), *The National Constitution and EU Law: The Principle of 'Supremacy'* [in Greek], Ant.N.Sakkoulas Publishers

Papakonstantinou E. (2006), Comment on Law 3471/2006, *Administrative Law Review*, 4 [in Greek], 442-446

Paraskevopoulos N. (2004), Security of the State and Legal Insecurity in: Maniatakis A. and Takis A. (eds.), *Terrorism and Human Rights* [in Greek], Savvalas Publishers

Pavlopoulos P. (2011), Speech during the Parliamentary Discussion of the Law Implementing the Data Retention Directive in Greece, Plenary Session Proceedings (10.02.2011) [in Greek] online at <http://www.hellenicparliament.gr/> last accessed 21.02.2011

Pateraki A. (2011), The Implementation of the Data Retention Directive: A Comparative Analysis in: Akrivopoulou C., Psygkas A. (eds.), *Personal Data Privacy & Protection in a Surveillance Era: Technologies & Practices*, IGI Global

Pinakidis G.(2007), The Obligatory Telecommunications Data Retention According to Directive 2006/24/EC Facing the European Convention of Human Rights Guarantees, *Hellenic Review of European Law*, 2 [in Greek], 405-438

Privacy International (2010, March 9), German Federal Constitutional Court Overturns Law on Data Retention, online at [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-566038](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-566038) – last accessed 23.12.2010

Rantos A. (1995), The Principle of Subsidiarity according to the Treaty on the EU, *Hellenic Review of European Law*, 1 [in Greek], 25-38

Skouris V. (1984), Civil Rights & the Census Case, *Armenopoulos*, 9 [in Greek], 689-694

Simitis Sp. (2010), Privacy –An Endless Debate?, *California Law Review*, 98, 1989-2005

Solove D. (2007), "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, *San Diego Law Review*, 44, 745-772

Sotiropoulos V. & Talidou Z. (2006), The Preventive Retention of Telecommunications Data for Crime-Combating Purposes (Directive 2006/24/EC), *Mass Media & Communication Law Review*, 2 [in Greek], 181-195

Tsatsos D. (2005), Security vs Freedom: The European Dimension in: Anthopoulos H., Contiades X. and Papatheodorou Th. (eds.), *Security & Human Rights in the Age of Risk* [in Greek], Ant.N.Sakkoulas Publishers

Tsiliotis H. (2006), The Threat of Human Rights by Modern Risks Emerging from Private Sources and the State's Obligation to Protect Them Through the Independent Administrative Authorities, *Administrative Law Review*, 4 [in Greek], 539-542

Tsiftoglou A. (2011), Surveillance in Public Spaces as a Means of Protecting Security: Questions of Legitimacy and Policy in: Akrivopoulou C., Psygkas A. (eds.), *Personal Data Privacy & Protection in a Surveillance Era: Technologies & Practices*, IGI Global

Tzanou M. (2011), Data Protection in EU Law: An Analysis of the EU Legal Framework and the ECJ Jurisprudence in: Akrivopoulou C., Psygkas A. (eds.), *Personal Data Privacy & Protection in a Surveillance Era: Technologies & Practices*, IGI Global

Tzalavra V. (2007), Preventive Surveillance of Electronic Communications for Crime Combating Purposes [1 BvR 668/04], *Criminal Chronicles*, NZ [in Greek], 565-569

Weinreb L. (2007), Responding to Terrorism - Lecture Given at the University of Athens, Greece on May 8<sup>th</sup> 2006, *Criminal Chronicles*, NZ [Greek translation], 481-487

# Enforceability of free/open source software licensing terms: a critical review of the global case - law

---

---

Thanos Tsingos

---

---

## 1. Introduction

When John Tukey first used the term “software” in a 1958 article in *American Mathematical Monthly*<sup>1</sup>, he could have probably never thought that almost fifty years after, a discernible sector, a huge industry around the world would be involved in and work on the production of such “software”. Indeed, the independent IT sector is nowadays so developed that it would not be exaggeration to say that - in economic terms - it demonstrates a considerable stability compared to all others, even under the dramatic conditions of a worldwide recession; it should be worth of noting that the worldwide software spending was a total \$232 billion in 2010, a 5.1 percent increase from 2009 and is expected to grow farther within 2011, since the impact of today’s recession on the software industry was quite tempered and not as dramatic as other IT markets<sup>2</sup>.

In the today’s world of computer programs one could possibly draw a useful – for our analysis - distinction between “proprietary software” and “free or open source” one, thereby distinguishing the relevant works depending on the “underlying copyright philosophy” of its creators<sup>3</sup>.

Traditional proprietary software is licensed through licensing agreements which usually define in detail what the licensee is permitted to do with respect to the licensed software. In those cases, the scope of the license is at most determined by the description of the acts that a licensee is entitled to proceed, since those acts constitute the very subject matter of the author’s exclusive economic rights granted under copyright law. Such licenses are “restrictive” in the sense that licensees are allowed to proceed to a few and precisely prescribed uses, the recitation of which is at the centre of the license; thus, any use of the software beyond the agreed ones, constitutes a copyright infringement under the applicable copyright law.

---

1. Wikipedia, online at: <[http://en.wikipedia.org/wiki/Software#cite\\_ref-2](http://en.wikipedia.org/wiki/Software#cite_ref-2)>.

2. Gartner, online at: <<http://www.gartner.com/it/page.jsp?id=1339013>>.

3. There are also other criteria according to which one could distinguish proprietary and non-proprietary software (e.g. price, characteristics etc), but for the purpose of our analysis we base such differentiation on the author’s will to license the software through one way or another.



However, that is not exactly the case with free/open source software. Here, the initial creator is willing to grant more freedom to its licensees by allowing more uses of the software, but he –together – sets forth certain conditions, under which such software may be further copied, modified, distributed etc. Contrary to proprietary licensing, the “heart” of a free/open source license is located on the consistent observance of those conditions on behalf of the licensee; such conditions may vary from mere attribution requirements to the strong “copyleft” clauses that every modification of the software must also be licensed under the same license terms as the initial one. The most important difference between those licensing schemes is that in free/open source software licenses the notion of “copyright infringement” is clearly peculiar: the distribution of the software without adhering to the “terms” and “conditions” of the free/open source license is pursued to constitute the copyright infringement.

The purpose of this contribution is to review the existing – at the time of writing - case law that deals with the specific issue of the validity and enforceability of such open source licensing terms and conditions from a copyright law point of view. The analysis is based on the self – evident fact that copyright laws may vary greatly across the world; thus, a detailed analysis of the copyright law system of each and every single State, in which the relevant judgements take place is inevitably not possible. Nevertheless, just the same, it proves to be true that there is an expanding case law that sets out the legal nature, the scope and the legal consequences of the existence of such terms and conditions within a free/open source license and its legal interrelation to copyright laws.

In this first part, we mention the basics about the computer software and the evolution of the free/open source software as a movement in the history of the IT industry. We then turn our discussion to the protection of computer programs by copyright, the traditional copyright licensing schemes and the newly introduced F/OSS licensing terms and conditions. In Part II, we offer a wide discussion on the existing case law with regard to the aforementioned legal issue of validity and enforceability of those F/OSS licensing terms, both in the USA and within the borders of the EU, in the factual context of each single case. Finally, in Part III a review of the existing case law will take place in terms of copyright, thereby comparing the legal approaches that seem to have followed by the two continents from which the jurisprudence derived: the USA and the EU and reaching to some useful conclusions thereto.

### ***1.1. Computer software***

There is no consensus on an absolute definition of what precisely is “computer software”. In general, it is commonly understood that a computer software is a set of programs, procedures, algorithms and related data along with its associ-

ated documentation that provide a computer with the required instructions, so that the latter would be able to perform a specific task.

In principle, a computer can only process tasks which are given in a binary form, the so-called “object code”. The object code is machine – readable in the sense that it contains a sequence of instructions that is almost unattainable for the human to understand. Thus, in order to program a computer, one needs to use a symbol or programming language<sup>4</sup>, that is, another computer program, on which a programmer writes his/her language statements (the “source code”). The programmer then runs a separate special program (the so-called compiler or interpreter)<sup>5</sup>, that processes those statements and turns them into (or interprets them into) “object code” that a computer’s processor uses and understands.

The reverse process of decompilation (translating the compiled code back to a semi-source code) is a part of a broader process of analyzing a computer program (reverse engineering). Such attempts of analyzing computer software can serve various purposes: it can provide information about the parts of a program, which take care of the interaction among the components of a system (interface purposes); it can be used for the production of a computer program that can work together with the decompiled program (interoperability purposes); it can provide the user of the program with assistance in making a code appropriate for a specific application or in removing errors (correction purposes); and finally it may enable a computer programmer to produce a competing software product (competitive purpose).

In the beginning of the computer era, the relevant market was focused on hardware producing. Large hardware producers generally provided computer programs free of charge, by “bundling” them with the hardware sold. In such a hardware – based industry, both professional and amateur programmers developed programs that were then deposited to “software pools”, which everyone could

---

4. Most computer programs have been written in “higher-level” program languages (such as Pascal, C, Prolog, Lisp and APL) as opposed to “low-level” ones, the distinction made upon the amount of abstraction between the language and machine language; in other words, “higher-level” program languages - as opposed to “low-level” ones - are human readable rather than computer readable, while low-level languages can be converted to machine code without using a compiler or interpreter and the resulting code runs directly on the processor.

5. While “compiling” and “interpreting” are the two main means by which programming languages are implemented, these are not fully distinct categories, one of the reasons being that most interpreting systems also perform some translation work, just like compilers. The terms «interpreted language» or «compiled language» merely mean that the canonical implementation of that language is an interpreter or a compiler; a high level language is basically an abstraction which is (ideally) independent of particular implementations. See also Bottis M., *Information Law*, 2004. (in Greek).

draw on free of charge. After a number of years it became clear that both these depositories were functioning below expectations and that the value of the software itself begun to increase as an independent and equally complementary tool of hardware, both working together to achieve a greater level of computer functionality (Buning, 2007).

It was not until June 23, 1969, when IBM, under pressure from a pending antitrust litigation by various competitors and the U.S. Department of Justice, announced that it would unbundle much of its software and services (Wikia, 2011). That is considered by many commentators as being the date, in which an independent software industry was born. The modernist commercial attitude of IBM in terms of its software along with the commercialization of its unprecedented “personal computers”, which replaced the old “mainframe” computers, put aside the “tailor made” computer programs that were used by the old computers, thereby creating a unique opportunity for the production of “computer software” of any kind and designed to serve various purposes (Bergin, 1970).

### ***1.2. The free/open Source software movement***

The history of the computer software development led the whole world to meet the need of legal protection (in the form of copyright), which inevitable led to a particular licensing scheme, also known as “proprietary software licensing”)<sup>6</sup>. Nevertheless, from 1983 to date two remarkable initiatives (namely the Free Software Foundation and the Open Source Initiative) started to challenge the notion of “proprietary software” and introduced the terms “Free Software” and “Open Source Software” correspondingly. As the founders inform us, these two terms do not actually refer to identical meaning. To understand the difference it would be useful to look into that history.

In 1983, when Richard Stallman, longtime member of the hacker community at the MIT Artificial Intelligence Laboratory, announced the GNU project, saying that he had become frustrated with the effects of the change in culture of the computer industry and its users. Software development for the GNU operating system began in January 1984, and the Free Software Foundation (FSF) was founded in October 1985. An article outlining the project and its goals was published in March 1985 titled the GNU Manifesto. The manifesto also focused heavily on the philosophy of free software. He developed “The Free Software Definition” and the concept of “copyleft”, designed to ensure software freedom for all.

---

6. See below.

According to the free software definition, free software is a matter of the users' freedom to run, copy, distribute, study, change and improve the software. More precisely, it means that the program's users have the four essential freedoms:

- The freedom to run the program, for any purpose (freedom 0).
- The freedom to study how the program works, and change it to make it do what (the user) wish (freedom 1). *Access to the source code* is a precondition for this.
- The freedom to redistribute copies so (the user) can help his/her neighbor (freedom 2).
- The freedom to distribute copies of his/her modified versions to others (freedom 3). By doing this (user) can give the whole community a chance to benefit from his/her changes. *Access to the source code* is a precondition for this<sup>7</sup>.

A program is free software if users have all of these freedoms. As implied by the definition itself, the term "free software" refers to freedom, not price.

However, not all of the users and developers of free software agreed with the goals of the free software movement. In 1998, a part of the free software community splintered off and began campaigning in the name of "open source." The term was originally proposed to avoid a possible misunderstanding of the term "free software," but it soon became associated with philosophical views quite different from those of the free software movement. Those views are reflected in a long "Open Source Definition"<sup>8</sup>, consisting of ten (10) articles formulated by the Open Source Initiative<sup>9</sup>, a California public benefit corporation.

In practice, nearly all open source software is free software. However, the two terms are used to express different underlying philosophies. As Richard Stallman, himself explains:

"... Open source is a development methodology; free software is a social movement. For the free software movement, free software is an ethical imperative, because only free software respects the users' freedom. By contrast, the philosophy of open source considers issues in terms of how to make software "better"-in a practical sense only. It says that non-free software is an inferior solution to the practical problem at hand. For the free software movement, however, non-free software is a social problem, and the solution is to stop using it and move to free software."

---

7. <<http://www.gnu.org/philosophy/free-sw.html>>.

8. <<http://www.opensource.org/docs/osd>>.

9. <<http://www.opensource.org/about>>.

From a legal point of view, it should be emphasized that the philosophical differences of those two initiatives are also reflected to the licenses that consider as certified to be applied to the software in question. To qualify as an “open source license” the license should cover computer software that qualifies as “open source” according to the open source definition. Similarly, a license is a “free software license”, if the covered program is intended to be used as “free” within the meaning of the free software definition<sup>10</sup>. As a result, a license may qualify as an “open source license” but not necessarily as a “free software license”<sup>11</sup>.

### ***1.3. Computer software and copyright***

The history of the legal protection of computer programs in the form of copyright is quite long. However, it is commonly understood that such protection is causally conjunct to the emergence of software, as an independent creation of the industry. In particular, the hardware independent production of software, taking place in early 70's, the increase in scale and the simple manner in which software – for businesses or for personal use – could be copied, all joined to create a strong need for legal protection of intellectual property rights among software producers (Buning, 2007, Bottis, 2004).

The choice of copyright as the appropriate means of legal protection of computer software was, though, a much questionable issue to be resolved. There was much discussion on whether computer software should be protected under patent, copyright law or under a sui generis approach. However, it was not until 1985, when a committee of experts convened jointly by WIPO and UNESCO “broke new ground” by choosing copyright as the appropriate means of protecting computer programs, simulating them to “literary” works within the meaning of Article 2(1) of the Berne Convention (WIPO, 2011). A few months later and the years after, many countries passed national copyright legislation covering computer software as literary works (e.g. the German Copyright Act - UrhG, 1985, the Dutch Copyright Act of 1994 following long – term case law etc)<sup>12</sup>.

It is widely accepted that copyright, as branch of intellectual property, is based on the notion of *exclusivity*. The holder of a copyright-protected work is granted by law with the exclusive authority to dispose his/her protected work “at will”.

---

10. It is important to note, however, that the FSF has approved as “free software” some licenses that are incompatible to the GNU GPL license.

11. By contrast, a license that qualifies as “free software”, is almost always understood to qualify as “open source”, since the criteria used by the OSD are a little looser than those provided for by the FSD.

12. It is worth noting that the United States of America was the first country to include software under the protection of the law by virtue of the “Software Copyright Act” enacted in 1980.

To implement such an exclusive freedom, law grants a copyright holder two fundamental “units” of rights: the moral rights and the economic ones. The first allow the respective owner to take certain actions to preserve the personal link between himself and the work while the latter allow the owner to derive financial reward from the use of his works by others.

Under moral rights, the owner is granted both the right to claim authorship of the work (sometimes called the right to “paternity”) and the right to object to any distortion, mutilation or other modification of, or other derogatory action, in relation to the work, which would be prejudicial to the author’s honour or reputation (sometimes called the right to “integrity”). Moral rights are only accorded to human authors and are independent of economic rights in the sense that remain with the author even after he has transferred his economic rights.

The set of exclusive economic rights (and thus every single componential exclusive right) is primarily defined by those acts that the owner would attempt on his own work expressing the abovementioned freedom of the owner, such as: the reproduction of the work (making copies)<sup>13</sup>; the public performance of the work; the broadcasting or other communication to the public of the work; the translation of the work; and the adaptation of the work. Each of those acts constitute the very subject-matter of corresponding exclusive rights granted to the owner under copyright (WIPO, 2011).

One of the most important international legislative instruments in the field of copyright is the Berne Convention on the protection of literary and artistic works its origins taking place back in 1886. This international Convention -last revised in 1971- prescribes the minimum standards to the copyright legislation of the members of the Berne Union and also includes the rule of national treatment. Nevertheless, none of its provisions relates to computer software as a copyright-protectable work (Szinger, 2001).

The first, however explicit reference to computer programs (software) as a work protected by copyright was made by virtue of Article 10 (1) of the World Trade Organization’s Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) of 1994, stating that “Computer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971)”<sup>14</sup>.

---

13. The reproduction right is the most basic right under copyright. That is the reason for which national laws recognize additional rights so that the basic reproduction right is respected e.g. the rights to authorize distribution, rental or importation of the copies of the protected work in question.

14. The TRIPS Agreement specifically incorporated Articles 1 through 21 of the Berne Convention into its Article 9. Moreover, the application of Article 6bis of the Berne Convention

This provision confirms that computer programs must be protected under copyright and that those provisions of the Berne Convention that apply to literary works shall be applied also to them. It confirms further, that the form in which a program is, whether in source or object code, does not affect the protection<sup>15</sup>. The obligation to protect computer programs as literary works means e.g. that only those limitations that are applicable to literary works may be applied to computer programs. It also confirms that the general term of protection of 50 years applies to computer programs. Possible shorter terms applicable to photographic works and works of applied art may not be applied.

Similarly, article 11 TRIPS provides that authors shall have in respect of at least computer programs the right to authorize or to prohibit the commercial rental to the public of originals or copies of their copyright works. However, the obligation does not apply to rentals where the program itself is not the essential object of the rental (WTO, 2011)<sup>16</sup>.

Article 9(2) of the TRIPS Agreement reiterates that copyright protection "... shall extend to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such"<sup>17</sup>. Without prejudice to the fact that the idea/expression dichotomy has been a much questionable matter of judicial review within the national borders of the States – contracting parties to TRIPS, it is generally acceptable that ideas, principles, algorithms or interfaces are excluded from the scope of copyright protection. On the contrary, the related documentation in any form, including application programs and operation systems shall fall within the ambit of copyright protection (Szinger, 2001; WIPO, 2011).

The normal prerequisite that a work must be original is well-suited to be applied to computer programs, as well. Although most routine programs consist of sub-routine elements, which often in themselves could hardly qualify as original

---

(with respect to moral rights) is guaranteed by virtue of Article 2.2 of the TRIPS Agreement (the safeguard clause), since said Article is not included by Reference in the TRIPS Agreement. All these mean that the provisions of the Berne Convention are incorporated into the TRIPS Agreement; that having as a further fundamental consequence that countries – contracting parties to TRIPS should carefully implement the relevant provisions of the Berne Convention, since they otherwise risk running afoul of their TRIPS obligations and becoming subject to the WTO dispute settlement procedure.

15. The rationale behind the law that object code must also be protected under copyright law is to grant the copyright holder with all respective exclusive rights against unauthorized decompilation.
16. <[http://www.wto.org/english/tratop\\_e/trips\\_e/intel2\\_e.htm](http://www.wto.org/english/tratop_e/trips_e/intel2_e.htm)>.
17. The wording of this provision is identical to that of Article 2 of the WIPO Copyright Treaty (WCT).

works, the combination of such elements and the structuring of the programs – with the exception of a few very simple programs – make them sufficiently creative (WIPO, 2011).

The above provisions of TRIPS with respect to computer programs were then supplemented by the subsequent provisions of the WIPO Copyright Treaty of 1996 (WCT) adopted by the WIPO Diplomatic Conference on Certain Copyright and Related Rights and Neighboring Rights Questions held the same year in Geneva<sup>18</sup>. This latter Treaty adopted similar provisions to those of the TRIPS Agreement in terms of copyright protection of computer programs. In particular, Article 4 of the WCT states that “Computer programs are protected as literary works within the meaning of Article 2 of the Berne Convention...” and that “Such protection applies to computer programs, whatever may be the mode or form of their expression.” It should be noted that the wording of this provision is slightly different from that of Article 10 (1) of the TRIPS Agreement (...whether in source or object code...). It is argued, however, that the text of Article 4 WCT is just less technology-specific, without that having the meaning of depriving from computer programs the protection accorded to them by the corresponding provision of Article 10 (1) of the TRIPS Agreement, since the scope of application of these two provisions is identical (WIPO, 2011)<sup>19</sup>. Moreover, in accordance to Article 11 TRIPS, Article 7 WCT reiterates that authors of computer programs shall enjoy the exclusive right of authorizing commercial rental to the public of the originals or copies of their works with the same exception, as outlined above.

In the framework of WCT, it is, indeed, of particular interest to note that a separate exclusive economic right is recognized in relation to computer programs. Article 6 (1) WCT provides the exclusive right of “distribution”, that is, “...of authorizing the making available to the public of the original and copies of ... works through sale or other transfer of ownership”, while the next paragraph of the same Article deals with the issue of its exhaustion. According to certain views, such a right (surviving at least until the first sale of copies) is an indispensable corollary to the right of reproduction recognized on this basis in many national jurisdictions, while other commentators consider that such an approach does not follow from the principles of many legal traditions around the world. In any case, WIPO considers it advisable to regard the provision of Article 6 (1) as containing “a Berne-plus-TRIPS-plus element” (WIPO, 2011)<sup>20</sup>.

---

18. By virtue of Article 1 (4) of WCT, contracting parties to that Treaty have to comply – *inter alia* – with Articles 1-21 of the Berne Convention.

19. Agreed statements concerning Article 4 of the WCT.

20. The Agreed Statements concerning Articles 6 and 7 WCT read: As used in these Articles, the expressions “copies” and “original and copies,” being subject to the right of distribution



Having outlined the international framework of copyright protection of computer programs, which sets forth the obligations of the States – contracting parties to these international agreements, one could possibly reach to the conclusion that, in short, a computer program is protected – in its “international” dimension- as a literary work within the meaning of the Berne Convention (Article 2 Berne, Article 10 (1) TRIPS, Article 4 WCT), while the author of such work further enjoys *both* the right to authorize or to prohibit the commercial rental to the public of originals or copies of the program in question (Article 11 TRIPS, Article 7 WCT) *and* the exclusive right of its “distribution” within the meaning of Article 6 (1) WCT.

#### ***1.4. Computer software licensing***

To grant a person with a permission to proceed to certain uses of the software concerned, it is widely accepted that a form of agreement is needed, where the contracting parties shall impress their will and will further define the terms and conditions, which govern their contractual relationship<sup>21</sup>. Such agreement typically takes the form of a written contract and is commonly known in the IT industry as a “software license”. Thus, a software license is required if the (end) user wishes to make use of a copy of the software, but where such a use would constitute copyright infringement of the software publisher’s exclusive rights under copyright law. In effect, the software license acts as a promise from the software publisher to not sue the end user for engaging in activities that would normally be considered as covered by exclusive rights belonging to the software publisher.

In licensing proprietary software, the software publisher grants a license to use one or more copies of software, but that ownership of those copies remains with the software publisher (hence use of the term “proprietary”). One consequence of this feature of proprietary software licenses is that virtually all rights regarding the software are reserved by the software publisher. Only a very limited set of well-defined rights are conceded to the end user. The most significant effect of this form of licensing is that, if ownership of the software remains with the software publisher, then the end user must accept the software license. In other

---

and the right of rental under the said Articles, refer exclusively to fixed copies that can be put into circulation as tangible objects. The question raised hereto was whether or not these Agreed Statements exclude the application of the right of distribution to transmissions in interactive digital networks, such as the Internet; the answer should be, though, negative, since the abovementioned statements determine only the minimum scope of the right of distribution. Contracting States may permissibly exceed it.

21. The word “contractual” and the relevant words “terms” and “conditions” should not give rise to any thought that the author distinguishes between a “license” and a “contract” or between “terms” and “conditions” of the license, since there is no intention to discuss such an “American law” issue in detail at this point of our analysis.

words, without acceptance of the license, the end user may not use the software at all (Madison, 2004). As such, it is typical of proprietary software license to include many terms which specifically prohibit certain uses of the software, often including uses which would otherwise be allowed under copyright law. As is usually the case with proprietary software licenses, they contain an extensive list of activities which are prohibited, such as reverse engineering, simultaneous use of the software by multiple users, and publication of benchmarks or performance tests<sup>22</sup>.

It follows that the conventional software licensing scheme is generally based on the notion of “pure exclusivity” under copyright law. So, traditional proprietary software is licensed through agreements which usually define in detail what the licensee is permitted to do with respect to the licensed software. In those cases, the scope of the license is at most determined by the description of the acts that a licensee is entitled to proceed, since those acts constitute the very subject matter of the author’s exclusive economic rights granted under copyright law. Such licenses are “restrictive” in the sense that licensees are allowed to proceed to a few and precisely prescribed uses, the recitation of which is at the centre of the license; thus, any use of the software beyond the agreed ones, constitutes a copyright infringement under the applicable copyright law.

### ***1.5. Free and open source software licensing***

In the context of the “proprietary software license”, copyright holders almost always license the “object code” of the computer program and not the “source code” itself (Madison, 2004). The source code in each and every copy of the computer program in question remains with the copyright holder, under the exclusivity of copyright law (proprietary). In the vast majority of the “proprietary software licenses”, there are clear terms against decompilation or other method of reverse engineering considering such actions as copyright infringements under the applicable law<sup>23</sup>.

Since the nature and the goal of the “proprietary software” had been challenged by the F/OSS proponents, it was almost impossible for lawyers not to meet a differentiated kind of a software license, other than the conventional one. In the

---

22. It would be outside the scope of this contribution to review the characteristics of a proprietary software license in depth with regard to copyright law. Nor is our intention to draw every single difference between a proprietary software license and a Free/Open Source one. What is important for our analysis is to point out of what the “metacentre” of a typical software license consist and compare it to the “copyright law” philosophy that settles in the architecture of F/OSS licenses. The result is valuable, since the notion of “copyright infringement” differentiates greatly from one to another licensing scheme.

23. Although that may not always be the case according to copyright laws.

relatively newly introduced F/OSS licensing regime, the initial creator is willing to grant more freedom to its licensees by allowing more uses of the software, but he –together – sets forth certain conditions, under which such software may be further copied, modified, distributed etc. Contrary to proprietary licensing, the “heart” of a free/open source license is located on the consistent observance of those conditions on behalf of the licensee; such conditions may vary from mere attribution requirements to the strong “copyleft” clauses that every modification of the software must also be licensed under the same license terms as the initial one. The most important difference between those licensing schemes is that in free/open source software licenses the notion of “copyright infringement” is clearly peculiar: the copying, modification and further distribution of the software without adhering to the “terms” and “conditions” of the free/open source license is pursued to constitute the copyright infringement.

Both the FSF and the OSI have approved numerous licenses that undoubtedly differ between themselves in many technical and legal respects. As already implied above, all “free software licenses” are OSI-certified but not all “open source licenses” may qualify as “free software ones”.

The classification of F/OSS licenses is indeed a very complex task depending on a large extent on which criterion is used to achieve it. A typical classification inevitably involves the way the so called “copyleft” concept appears in the F/OSS license in question.

The actual word ‘copyleft’ has no legal meaning in itself, it is simply a play on the word ‘copyright’. It describes the practice of using copyright law to remove restrictions on distributing copies and modified versions of a work for others and requiring that the same freedoms be preserved in any modified versions. An author may, through a copyleft licensing scheme, give every person who receives a copy of a work permission to reproduce, adapt or distribute the work as long as any resulting copies or adaptations are also bound by the same copyleft licensing scheme. For this reason copyleft licenses are also known as reciprocal licenses. Copyleft licenses are also conditional licenses. One of the conditions licensee must satisfy before distributing copylefted software is that any changes he makes to that software be likewise released under the copylefted license. A copyleft license ensures that all modified versions of the project remain free in the same way.

It should, however be noted that the concept of “copyleft” relies on the basic principles of copyright (Reidenberg, 2007). Whereas copyright law has traditionally been used to withhold permission to copy, modify or distribute software, some licenses instead use copyright law to require that such permissions be granted. Such licenses are said to keep code “forever free” (SFLC, 2008). It is sometimes said that while a copyright generally enables a person to claim “all rights reserved”, a copyl-

eft generally means “some rights reserved”. Although this is not a legal terms and it carries no legal significance, it is one of the central terms in the hacker community to denote their discontent with copyright laws (Brown, 2010).

F/OSS licenses can have stronger, weaker or no copyleft provisions, thereby distinguishing between the so –called “Academic” or “permissive” or “BSD-Style” licenses, which are generally understood to permit recipients to release modified versions under more restrictive terms (including both proprietary and copyleft terms)<sup>24</sup>, and the “strong copyleft” licenses like the GPL which prioritize ensuring that all downstream recipients receive source code and permission to modify the software (Laurent, 2010).

The GPL (v.2 and newly released v.3<sup>25</sup>) is an example of a “strong copyleft” license and may serve as a basis for understanding the “copyleft” concept within a F/OSS license. These licenses may contain: a requirement that the licensee publish or make available for any works based on or derived from the original software, a requirement that the licensee send the sponsoring open-source community a copy of all versions of derivative software using the software and a requirement that a licensee make the software documentation available at no charge (Lee, 2010).

By contrast, weak copyleft licenses permit the licensee to include or link to the original, unmodified code in a greater work without being required to license the entirety of the new work under the open source license, as it is the case with Mozilla Public License (MPL), the Eclipse Public License (EPL) and the Artistic License (Lee, 2010).

At last there are FOSS licenses with no “copyleft” provisions at all, such as the Free BSD, the University of California and the Apache License. These “permissive” licenses are restricted in requiring the mere provision of the appropriate copyright notices, attribution information etc. (Armstrong, 2010). Thus, they are usually known as “attribution Licenses”.

---

24. These licenses guarantee the availability of their permissions only for the first generation of the software.

25. See in that regard the relevant works of: Douglas A. Hass, “The gentlemen’s agreement soldiers on, Linux under GNU, General Public Licenses 2 and 3”, online at: <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1330020](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1330020)>, last accessed 26.03.2011, Robert W. Gomulkiewicz, (2007) “A first look at general Public License 3.0, The Computer and Internet Lawyer”, vol.24, no. 11, and Andres Guatamuz Gonzalez, (2006), “GNU General Public License v.3: a legal analysis”, Script-Ed, Vol. 3, Issue 2.

## 2. Validity and enforceability of F/OSS licensing terms - expanding case-law

In this part, we attempt to provide an analysis of the existing – as of the date of writing – case law that interpret both many F/OSS licensing terms and describe the F/OSS phenomenon in legal terms. Starting with the country that first incorporated legislation to protect computer software under copyright (U.S.A.), we then turn our discussion to the case law presented in some European Union Countries (namely Germany and France). As an initial observation, one should bear in mind that we analyse case law of different jurisdictions, which means in effect that copyright laws may vary greatly. However, just the same, such analysis should be understood as a starting point for further discussion regarding the validity and enforceability of F/OSS licensing terms in terms of copyright.

### 2.1. U.S. Case Law

It might be true that USA was the first State in the world to include computer programs into its copyright legislation, however, it was not the first to produce detailed case law regarding the legal issue of whether certain F/OSS licensing terms and conditions are valid and enforceable. Anyway, it is important to note that within the US Jurisdiction there have been extensive discussions of whether F/OSS licenses themselves constitute a contract or a license. This “contract/license” debate is discussed in the next part, after having outlined the history of the relevant case law.

#### i) Progress Software Corp. v. MySQL AB

One of the first US cases to address GPL validity was *Progress Software Corp. v. MySQL AB*. In 2001, MySQL sued Progress Software for allegedly distributing a database product that linked directly to MySQL code (which had originally been released under the GPL), without distributing the source code for the database product. According to the GPL, under certain circumstances, if a second program is linked to a GPL program, the source code distribution requirements may apply to the linked program, as well. MySQL sought a preliminary injunction to prevent Progress Software from distributing its database programs during the trial. Ruling on this injunction, U.S. District Judge Patti B. Saris treated the GPL as an enforceable and binding license. Judge Saris, however, did not issue the injunction, noting that there were questions as to whether Progress’ software was a derivative or independent work under the GPL (that is, whether the source code distribution requirements applied to that work). The case was eventually settled out of court without any further guidance from the Court.

## ii) Planetary Motion, Inc. v. Techplosion, Inc.

An interpretation of the GNU GPL was also considered tangentially in *Planetary Motion, Inc. v. Techplosion, Inc.*<sup>26</sup>. In that case, the Appellee Planetary Motion sued Techsplosion for infringement and dilution of an unregistered trademark associated with computer software, which was distributed without charge to users pursuant to a GNU General Public License. In an attempt to support its finding of ownership, the Appellate Panel noted:

“...Appellants misconstrue the function of a GNU General Public License. Software distributed pursuant to such a license is *not necessarily ceded to the public domain* and the licensor purports to retain ownership rights, which may or may not include rights to a mark”<sup>27</sup>.

## iii) Daniel Wallace v. Free Software Foundation, Inc.

In 2005, David Wallace filed a complaint against Free Software Foundation that the latter unlawfully conspired with its distributors to fix prices of computer programs in violation of the US Sherman Act. In the relevant antitrust case, also known as *Daniel Wallace v. Free Software Foundation, Inc.*<sup>28</sup>, the Court held (in its initial grant of summary judgement in favour of the FSF), that the GPL is a vertical agreement (meaning it is an agreement among different levels of users within the same chain of distribution) and as such, cannot alone form the basis of a per se violation of U.S. antitrust laws. Finally, Judge John D. Tinder, after dismissing the Fourth Amended Complaint of the plaintiff under the U.S. Federal Rule of Civil Procedure, and with respect to the GPL as a license itself, stated:

“...The court’s understanding from the GPL itself is that it is a software licensing agreement through which the GNU/Linux operating system may be licensed and distributed to individual users so long as those users “cause any work that (they) distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.” (GPL 3.) The GPL purportedly functions to “guarantee (users’) freedom to share and change free software.” (GPL Preamble.) As alleged, the GPL in no way forecloses other operating systems from entering the market. Instead, it merely acts as a means by which certain software may be copied, modified and redistributed without

---

26. *Planetary Motion, Inc. v. Techplosion Inc.*, (2001), Court Of Appeals For The 11th Circuit, 261 F.3d 1188.

27. At para. 23.

28. *Daniel Wallace v. Free Software Foundation, Inc.*, (2005), U.S. District Court, Southern District of Indiana, Indianapolis Division, 31728, 7 - 8.

violating the software's copyright protection. As such, the GPL encourages, rather than discourages, free competition and the distribution of computer operating systems, the benefits of which directly pass to consumers"<sup>29</sup>.

#### **iv) Daniel Wallace v. International Business Machines Corporation, Red Hat, Inc. and Novell, Inc.**

The next year, Daniel Wallace filed a new lawsuit against the software companies IBM, Novell, and Red Hat, who profit from the distribution of open-source software, specifically the GNU/Linux operating system. Wallace's allegation was that these software companies were again engaging in anticompetitive price fixing. Judge Richard L. Young dismissed the case on May 16, 2006 on the same – as the above – procedural law grounds. Wallace then filed an appeal in the Seventh Circuit Appeal Court, where his case was heard *de novo* in front of a three-judge panel. Wallace lost his appeal, with the judge citing a number of problems with his complaint. Although the Court's ruling in this case (*Daniel Wallace v. International Business Machines Corporation, Red Hat, Inc. and Novell, Inc.*)<sup>30</sup>, is basically focused on antitrust concerns, it, however, seems to provide *some* guidance as to the issue of whether the GPL is a legal binding and enforceable licensing agreement. Judge Frank Easterbrook – delivering the opinion of the Court – stated, respectively:

“Authors, who distribute their works under this license, devised by the Free Software Foundation, Inc., authorize not only copying but also the creation of derivative works – and the license prohibits charging for the derivative work. People may make and distribute derivative works, if and only if they come under the same license terms as the original work. Thus, the GPL propagates from user to user and revision to revision: neither the original author, nor any creator of a revised or improved version, may charge for the software or allow any successor to charge. Copyright law, usually the basis of limiting reproduction in order to collect a fee, ensures that open-source software remains free: any attempt to sell a derivative work will violate the copyright laws, even if the improver has not accepted the GPL. The Free Software Foundation calls the result “copyleft””.

#### **v) SCO Group, Inc. v. IBM**

For the purpose of our analysis it would be an omission not to mention the pending *SCO Group, Inc. v. IBM*<sup>31</sup> litigation. On March 6, 2003, the SCO Group (formerly known as Caldera Systems) filed a \$1 billion lawsuit in the US against IBM

---

29. At para 5 and 6.

30. *Daniel Wallace v. International Business Machines Corporation, Red Hat, Inc. and Novell, Inc.* (2006), Court of Appeals for the 7<sup>th</sup> Circuit, 467 F.3d 1104.

31. *SCO Group, Inc. V. IBM*, Civil action No 2:03cv0294.

for allegedly “devaluing” its version of the UNIX operating system. SCO claimed that IBM had, without authorization, included portions of SCO’s proprietary Unix code in IBM’s open source Linux product. Open source proponents including FSF and the Open Source Initiative, have criticized SCO’s case. To date SCO has refused to publicly identify source code at issue. A significant, however, issue in this litigation relates to whether SCO actually owns the copyright to the Unix Code in question. This issue has been the very subject matter of another case, namely that of *SCO Group, Inc. v. Novell*<sup>32</sup>. Moreover, in an order entered on 21 September 2007, Judge Kimball administratively closed the case of *SCO v. IBM* due to SCO filing for bankruptcy on 14 September 2007. This means that all action in *SCO v. IBM* is stayed until SCO emerges from bankruptcy proceedings. If and when it does, the case *SCO v. IBM* will resume where it left off (Groklaw, 2007).

With respect to that other litigation of *SCO Group, Inc. v. Novell*, it should be mentioned that on August 24, 2009, the U.S. Court of Appeals for the Tenth Circuit reversed the portion of the August 10, 2007 district court summary judgment that Novell owned the copyright to Unix<sup>33</sup>. As a result, SCO was permitted to pursue its claim of ownership of the Unix copyrights at trial. However, on March 30, 2010 the jury returned a verdict, finding that Novell owns the copyrights.

There is no further development in the case of *SCO v. IBM*, due to the involvement of SCO Group in bankruptcy proceedings, even though the preliminary question on whether SCO actually owns the copyright to the Unix Code at issue has already been answered negatively due to the findings in *SCO Group, Inc. v. Novell*. In any case, the still pending *SCO Group v. IBM* has the potential to provide additional judicial direction on the enforceability of the GPL (Gatto, 2007).

#### **vi) Robert Jacobsen v. Matthew Katzer and Kamind Associates, Inc**

Undoubtedly, the recognition of a F/OSS license as an enforceable licensing agreement in terms of copyright law was well-established for first in the history of the US case law in *Robert Jacobsen v. Matthew Katzer and Kamind Associates, Inc*<sup>34</sup>. The facts of the case were as follows:

Jacobsen managed an open source software group called Java Model Railroad Interface (“JMRI”). Through the collective work of many participants, JMRI created a computer programming application called DecoderPro, which allowed model railroad enthusiasts to use their computers to program the decoder chips that

---

32. *SCO Group, Inc. v. Novell*, Civil Action No 2:04cv139.

33. *SCO Group, Inc. v. Novell, Inc.* (2009), Court of Appeals for the 10<sup>th</sup> Circuit, No. 08-4217.

34. *Robert Jacobsen v. Matthew Katzer and Kamind Associates, Inc.*, (2008), Court of Appeals for the Federal Circuit, 535 F.3d 1373.



control model trains. DecoderPro files were available for download and use by the public free of charge from an open source incubator website called SourceForge; Jacobsen maintains the JMRI site on SourceForge. The downloadable files contained copyright notices and referred the user to a "COPYING" file, which clearly set forth the terms of the Artistic License. On the other side Katzer/Kamind offered a competing software product, Decoder Commander, which was also used to program decoder chips. During development of Decoder Commander, one of Katzer/Kamind's predecessors or employees was alleged to have downloaded the decoder definition files from DecoderPro and used portions of these files as part of the Decoder Commander software. The Decoder Commander software files that used DecoderPro definition files did not comply with the terms of the Artistic License. Specifically, the Decoder Commander software did not include (1) the authors' names, (2) JMRI copyright notices, (3) references to the COPYING file, (4) an identification of SourceForge or JMRI as the original source of the definition files, and (5) a description of how the files or computer code had been changed from the original source code. The Decoder Commander software also changed various computer file names of DecoderPro files without providing a reference to the original JMRI files or information on where to get the Standard Version.

Jacobsen brought an action for copyright infringement and moved for a preliminary injunction. The District Court held that the open source Artistic License created an "intentionally broad" nonexclusive license which was unlimited in scope and thus did not create liability for copyright infringement<sup>35</sup>. The District Court found that Jacobsen had a cause of action only for breach of contract, rather than an action for copyright infringement based on a breach of the conditions of the Artistic License. Because a breach of contract creates no presumption of irreparable harm, the District Court denied the motion for a preliminary injunction. On appeal, the Court reversed the District Court's order on several grounds.

---

35. The District Court's reasoning in *Jacobsen v. Katzer* ((2007), U.S. Dist. LEXIS 63568, 2007 WL 2358628, at para 7)) was as follows:

"...The plaintiff claimed that by modifying the software the defendant had exceeded the scope of the license and therefore infringed the copyright. Here, however, the JMRI Project license provides that a user may copy the files verbatim or may otherwise modify the material in any way, including as part of a larger, possibly commercial software distribution. The license explicitly gives the users of the material, any member of the public, "the right to use and distribute the (material) in a more-or-less customary fashion, plus the right to make reasonable accommodations." The scope of the nonexclusive license is, therefore, intentionally broad. The condition that the user insert a prominent notice of attribution does not limit the scope of the license. Rather, Defendants' alleged violation of the conditions of the license may have constituted a breach of the nonexclusive license, but does not create liability for copyright infringement where it would not otherwise exist."

At a first place, the Court noted that several types of public licenses often referred to as “open source” licenses have been designed to provide creators of copyrighted materials with a means to protect and control their copyrights. In explaining the underlying philosophy of an open source project and citing *David Wallace v. IBM Corp.* (with respect to the function of a GNU-GPL licensed project) it stated:

“Open Source software projects invite computer programmers from around the world to view software code and make changes and improvements to it. Through such collaboration, software programs can often be written and debugged faster and at lower cost than if the copyright holder were required to do all of the work independently. In exchange and in consideration for this collaborative work, the copyright holder permits users to copy, modify and distribute the software code subject to conditions that serve to protect downstream users and to keep the code accessible. By requiring that users copy and restate the license and attribution information, a copyright holder can ensure that recipients of the redistributed computer code know the identity of the owner as well as the scope of the license granted by the original owner. The Artistic License in this case also requires that changes to the computer code be tracked so that downstream users know what part of the computer code is the original code created by the copyright holder and what part has been newly added or altered by another collaborator.”

The Court also reiterated the economic motives inherent in public licenses citing in that regard the respective recognition by the Court in *Planetary Motion, Inc. v. Techsplosion, Inc.* It noted, however, that there were two main issues to be evaluated, the first being whether the terms of the Artistic License are conditions of, or merely covenants to, the copyright license and whether the use by Katzer/Kamind was outside the scope of the license. If the answer to the first question was affirmative then the Court should proceed to the second and only if it is found that the use by defendants is outside the scope of the license, then the plaintiff is entitled to remedies due to a copyright infringement.

Citing the established case-law, the Court of Appeals mentioned that generally, a “copyright owner who grants a nonexclusive license to use his copyrighted material waives his right to sue the licensee for copyright infringement” and can sue only for breach of contract<sup>36</sup>. If, however, a license is limited in scope and the licensee acts outside the scope, the licensor can bring an action for copyright infringement<sup>37</sup>. Thus, if the terms of the Artistic License allegedly violated are both

---

36. *Sun Microsystems, Inc., v. Microsoft Corp.*, (1999), 9<sup>th</sup> Circuit, 188 F.3d 1115, 1121; *Graham v. James*, 2<sup>nd</sup> Circuit, 144 F.3d 229, 236.

37. *S.O.S., Inc. v. Payday, Inc.*, (1989) 9<sup>th</sup> Circuit, 886 F.2d 1081, 1087; Nimmer on Copyright, § 1015(A) (1999).

covenants and conditions, they may serve to limit the scope of the license and are governed by copyright law. If they are merely covenants, by contrast, they are governed by contract law<sup>38</sup>.

To identify whether the terms of the Artistic License serve as conditions of the license, which in turn limit its scope, or as a mere covenant, the Court used consecutively two generally acceptable and well-known approaches of interpreting the law (here, the terms of the License): the “linguistic” interpretation and the “teleological” one.

As to the language of the License the Court rules:

“...The Artistic License states on its face that the document creates conditions: “The intent of this document is to state the *conditions* under which a Package may be copied.” (Emphasis added.) The Artistic License also uses the traditional language of conditions by noting that the rights to copy, modify, and distribute are granted “*provided that*” the conditions are met. Under California contract law, “provided that” typically denotes a condition. *See, e.g., Di-epenbrock v. Luiz*, 159 Cal. 716, 115 P. 743 (1911)...”

The brief, though, interpretative reference to the language of the Artistic License as such, was then eagerly followed by a long and quite thoughtful teleological approach of the License as a means to achieve the goal of an open source project:

The conditions set forth in the Artistic License are vital to enable the copyright holder to retain the ability to benefit from the work of downstream users. By requiring that users who modify or distribute the copyrighted material retain the reference to the original source files, downstream users are directed to Jacobsen’s website. Thus, downstream users know about the collaborative effort to improve and expand the SourceForge project once they learn of the “upstream” project from a “downstream” distribution, and they may join in that effort... The copyright holder here expressly stated the terms upon which the right to modify and distribute the material depended and invited direct contact if a downloader wished to negotiate other terms. These restrictions were both clear and necessary to accomplish the objectives of the open source licensing collaboration, including economic benefit.... Through this controlled spread of information, the copyright holder gains creative collaborators to the open source project; by requiring that

---

38. *Graham*, 144 F.3d at 236-37 (whether breach of license is actionable as copyright infringement or breach of contract turns on whether provision breached is condition of the license, or mere covenant); *Sun Microsystems*, 188 F.3d at 1121 (following *Graham*; independent covenant does not limit scope of copyright license). In *Jacobsen*, the District Court, clearly treated the license limitations as contractual covenants rather than conditions of the copyright license.

changes made by downstream users be visible to the copyright holder and others, the copyright holder learns about the uses for his software and gains others' knowledge that can be used to advance future software releases..."

In verifying the limited scope of the Artistic License, in particular, the Court notes:

"...In this case, a user...is authorized to make modifications and to distribute the materials "provided that" the user follows the restrictive terms of the Artistic License. A copyright holder can grant the right to make certain modifications, yet retain his right to prevent other modifications. Indeed, such a goal is exactly the purpose of adding conditions to a license grant. The Artistic License, like many other common copyright licenses, requires that any copies that are distributed contain the copyright notices and the COPYING file...The clear language of the Artistic License creates conditions to protect the economic rights at issue in the granting of a public license. These conditions govern the rights to modify and distribute the computer programs..."

After concluding that the Artistic License sets forth conditions (and not mere covenants) upon which a licensee may further copy and distribute the copyrighted material (and, therefore, such a non-exclusive license is limited in scope), it was relatively easy for the Court to further conclude that the defendant acted outside the scope of the license.

The ruling of the Court of Appeals in *Jacobsen v. Katzer* has been of crucial importance in placing a F/OSS license into the generality of the copyright law system, as well. In a persuasive language the Court explains:

"...Copyright holders who engage in open source licensing have the right to control the modification and distribution of copyrighted material... Copyright licenses are designed to support the right to exclude; money damages alone do not support or enforce that right. The choice to exact consideration in the form of compliance with the open source requirements of disclosure and explanation of changes, rather than as a dollar-denominated fee, is entitled to no less legal recognition. Indeed, because a calculation of damages is inherently speculative, these types of license restrictions might well be rendered meaningless absent the ability to enforce through injunctive relief...The attribution and modification transparency requirements directly serve to drive traffic to the open source incubation page and to inform downstream users of the project, which is a significant economic goal of the copyright holder that the law will enforce..."

The judgment of the Court of Appeals in *Jacobsen v. Katzer* has been the first case in the history of the U.S. case law to address legal issues regarding the Artistic license as OSI – certified. Before analyzing any concern by virtue of the American

case-law in terms of copyright, we proceed in reviewing the corresponding case-law in Europe.

## **2.2. European Case Law**

While European Countries would be assumed to present F/OSS case-law chronologically after the USA, this is not the case. Internationally, Germany has developed a remarkable body of case law in relation to the issues of enforceability of the F/OSS license terms. This is primary due to the activity of Harald Welte, a German citizen and one of the most active proponents of the GPL in Europe. Having established the [gpl-violations.org](http://gpl-violations.org), an organization collecting reports of violations of GNU GPL license, he has brought successfully before the Courts numerous legal actions against potential violators of the GPL licensed projects. In this sub-part we mention four decisions of German Courts due to Welte's activity ((i) – (iv)) and two more decisions derived from French Courts ((v) – (vi)).

### **i) Harald Welte v. S(itecom) Deutschland GmbH**

In *Harald Welte v. S(itecom) Deutschland GmbH*<sup>39</sup>, a Munich Court had the opportunity to address the enforceability of several GPL (v. 2) terms, thus being the first European national Court to consider the validity and enforceability of such a license.

In that case, plaintiff Harald Welte was a member of the open source project “netfilter/iptables” and as a so-called “maintainer” chiefly responsible for the development of the program. Since 2001, plaintiff was the maintainer of a team that operated the Internet platform “[www.netfilter.org](http://www.netfilter.org)”, on which the software “netfilter/iptables” was offered for download in source-code form and made available to members of the team and others for further development. The software “netfilter/iptables” was an integral building part of the widespread operating system GNU/Linux and - as indicated on the Internet page - was a Free Software that could be used by everybody under the conditions of the GNU General Public License version 2.0 (GPL). Defendant Sitecom advertised and distribute through the website [www.sitecom.com](http://www.sitecom.com), on which some software available for download free-of-charge contained the software “netfilter/iptables” in object-code form, which plaintiff programmed himself in its entirety. On the website of the company s(itecom), however, there was neither a hint to the fact that the firmware also contained software that has been put under the GNU General Public License, nor a reference to the license text of the GPL or the source code of the software “netfilter/iptables”, in violation of the GPL terms.

---

39. *Harald Welte v. S(itecom) Deutschland GmbH*, (2004) District Court München I file number: 21 O 6123/04.

Plaintiff Harald Welte, demanded from defendant to restrain from the GPL violations and, when defendant refused to certify their future restraining, plaintiff filed suit on 1 April 2004 and requested issuance of a preliminary injunction.

The court, following the request, issued the following preliminary injunction:

“...1. Defendant is forbidden, under penalty ...to distribute and/or copy and/or make publicly accessible the software “iptables/netfilter”, without pointing to the licensing under the GPL and attaching the license text of the GPL and making the source code of the software “netfilter/iptables” available free of license fees, according to the conditions of the GNU General Public License, Version 2 (GPL).”

Defendant appealed the preliminary injunction. On appeal, the Munich Court had to address a number of issues raised by the parties. The most important, however, issue to be discussed was the validity of section 4 of the GPL (v.2.)<sup>40</sup>.

In an attempt to analyze the GPL terms (section 4 in particular) in the framework of German law, the Court noted, in a first place, that being entitled to a disposition pertaining to par. 97 UrhG requires that defendant has not received usage rights for the software. Regarding an infringement of rights, two alternatives can be distinguished; first, that defendant has never received rights of use, and second, that the rights of use once received have terminated according to section 4 GPL.

Concerning the first alternative, it is imaginable that no effective agreement had been reached because of invalid general conditions of sale<sup>41</sup>. In considering that, the Court further noted that, given the facts of the case and with strict accordance to the German law, the license conditions (treated as general conditions of sale) had been effectively included into a potential contract between defendant and plaintiff<sup>42</sup>.

---

40. Section 4 GPL (v.2) reads:

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.”

41. At para. 306 section 2 BGB (Bürgerliches Gesetzbuch = Civil Code). Moreover, the court considered the license conditions as general conditions of sale that are to be checked according to par. 305 ff. BGB.

42. According to par. 305 section 2 BGB.

Since a potential contract had been concluded between the parties concerned, the Court should consider the validity of the GPL terms in the second alternative (the rights of use once received have terminated) according to the German Law, in particular with regard to the provision of 307 BGB. That provision encompasses the “fairness test”, a norm originated from the implementation of European Council Directive 93/13 on unfair terms in consumer contracts into the national (German) legislation. The provision of 307 Abs 2 Nr 1 BGB foresees in particular that a provision is invalid if it cannot be reconciled with essential basic principles of the statutory rule from which it derives.

Starting from section 4 GPL the Court had to establish whether such term (as containing a resolutive condition with in rem effect) is a permissible limitation of usage rights according to German law<sup>43</sup>. Even though it was found that section 4 GPL did not qualify as such, it was however of significant importance for the Court to declare that “...the literature endeavors legal constructions in order to make the automatic termination of rights that is described in number 2 (GPL) legally effective also on the territory of the Federal Republic of Germany”<sup>44</sup>. Such a legal construction, of which the plaintiff had been a keen proponent, suggested assuming only an in rem agreement with conditional annulment, which prescribes an automatic termination in case the licensee does not adhere to the contract duties. The argument presented was that such object-related legal transactions are in principle not adverse to conditions. The Court found such an approach compatible with the German law<sup>45</sup> on several grounds.

In a first place, the Court ruled that the legal effects of a permissible limitation or an automatic termination upon violation of certain contract duties can both lead to the same legal consequences, because there is no ownership of usage rights in both cases and potential dispositions with third parties would be void due to lack of authority.

In a second place it considered, however, the question of whether such a solution serves to circumvent the regulations of par. 31 UrhG in some cases. With regard

---

43. According to par. 31 section 1 sentence 2 UrhG. The relevant paragraph reads (in unofficial English translation):

“Paragraph 31 section 1 and 2: Granting Usage Rights

1) The author can grant others the right to use the work in some or all manners (usage right). The usage right can be granted as a simple or exclusive right and can be limited geographically, temporally, or content-wise.

2) The simple usage right allows the owner to use the work as permitted, without excluding the use by others.”

44. In unofficial English translation.

45. In particular with par. 31 section 1 sentence 2 UrhG.

to that question the Judges noted that, first of all, it does not follow (from the language of par. 31 UrhG) that transfers of copyright-related usage rights with conditional annulment are excluded in general. The question whether such a condition is legally permissible, i.e. implements a circumvention of par. 31 UrhG or not, is logically associated to the question of which effects the annulment condition could have on the fitness for sale of the rights or the (further modified) objects that the software has been applied to. Maintaining the fitness for sale of the rights, in particular in a multi-level vendor chain, essentially presupposes that not every violation against some duties results in the software being copied and/or distributed by unauthorized parties. This is particularly true in the case of GPL, since both the respective license grants for third parties are not terminated as long as they accept and comply with the GPL conditions and such third parties can at any time obtain the necessary usage rights from the author directly upon acceptance of the GPL. So, the consequences of a termination of rights predominantly affect only the contractor of the author, similar to a liability-based limitation, thus the fitness for sale of the rights is only marginally impaired. Even the automatic termination is not particularly severe for the violator, because the latter can reacquire the rights at any time by acceptance of and compliance with the conditions of the GPL. Thus, the Court opined that section 4 GPL does not constitute a circumvention of par. 31 section 1 sentence 2 UrhG.

In a third place, the Court noted that even if the objections regarding the permissibility of number 4 sentences 2 and 3 GPL applied, that would not cause number 4 sentence 1 GPL to become invalid. The clause would only be partially invalid, with the consequence that a violation of number 4 sentence 1 GPL would only have liability effects as to the violator alone. Besides, the legislation itself, seems to take into account the notion of open source software. The Court, exercising in that regard its explanatory power, states:

“...the legislator expressly recognizes the fundamental principle of open source software with the provision in par. 32 section 3 sentence 3 UrhG”<sup>46</sup>.

In a final place, the Court shared the view of the plaintiff that even if section 4 GPL or section 3 would be invalid because the contract as a whole had never be

---

46. par. 32 UrhG reads:

“Paragraph 32: Adequate Compensation

(1)...

(2)...

(3) A contract partner cannot rely on an agreement that differs from the sections 1 and 2 to the disadvantage of the author. These rules also apply if they are circumvented by other means. However, the author can grant a usage right for everybody free of charge.” (emphasis added).



legally concluded between the parties, there are reasons to assume that no effective agreement has been reached, with the consequence that *any use of the software is illegal*.

## ii) Harald Welte v. D-Link

The final judgement of the Munich Court in *Harald Welte v. S(itecom) Deutschland GmbH* had an impact in the subsequent case law of the German jurisprudence. In 2006 another German Court also had the opportunity to address issues of validity and enforceability of the GPL terms in *Harald Welte v. D-Link*<sup>47</sup>. In that case, said Plaintiff had been a lawful assignee of three computer programs (“msdosfs”, “initrd” and “mtd”), which were parts of the Linux-kernel and licensed (by Plaintiff) under the GNU General Public License v. 2.0 exclusively. Similarly to the facts of the previous case, Defendant (a subsidiary company of a Taiwanese manufacturer), distributed a data storage unit (containing the said programs) in violation of the GPL conditions, since the licence text of the GPL was not enclosed, a disclaimer of warranty was not made, and the source code was not disclosed either.

In a very similar but more unequivocal thinking, the Court after citing *Harald Welte v. S(itecom)* made some remarkable observations.

In a first place it thought that the GPL applies to the legal relationship between the authors and Defendant. In the case of free software it is to be assumed that the copyright holder by putting the program under the GPL makes an offer to a determinable or definite circle of people and that this offer is accepted by users (of the software) through an act that requires consent under copyright law; in this respect, it can be assumed that the copyright holder enters into this legal relationship without receiving an actual declaration of acceptance according to Section 151 of the German Civil Code (BGB). The conditions of the license granted under the GPL must be regarded as standard terms and conditions that are subject to Sections 305 et seq. of the German Civil Code (BGB). Since the conditions of the license granted by the GPL are easily available on the Internet, they were without a doubt incorporated into the contractual relationship between the authors and Defendant (Section 305, Subsection 2, No.2 of the German Civil Code (BGB)).

In addressing the issue of the validity of section 4 of the GPL the Court noted that - pursuant to that provision - the rights under the GPL are terminated and revert to the author if the user does not publish a disclaimer of warranty on each copy (of the program), make reference to the GPL, accompany the program with the license text, and provide the source code of the program according to Sec. 2 of the GPL. These rules do not unduly discriminate the user and are therefore not

---

47. *Harald Welte v. D-Link*, (2006), District Court of Frankfurt am Main 2-6 0 224/06.

invalid pursuant to Section 307, Subsection 2 No. 1 of the German Civil Code (BGB). The Court, however, pointed out that the obligations set forth by section 2 GPL are not –according to established case law – a valid limitation of the right to use under Section 31, Subsection 1, Sentence 2 of the German Copyright Act (UrhG), but they must be understood to provide that the grant of the non-exclusive right of use under the GPL is subject to the condition subsequent (Section 158 of the German Civil Code (BGB)) that the licensee must not fail to comply with the terms of the agreement. Upon occurrence of the condition the license (granted under the GPL) is terminated.

The Court also considered that this legal construction offered by the GPL (terminating the agreement pursuant to section 4 if licensee does not comply to its duties prescribed in section 2) does not circumvent Section 31 of the German Copyright Act (UrhG), because it does not severely affect the marketability of the rights or the physical copies of the work<sup>48</sup>. Thus, since Defendant violated the obligations provided for in Sec. 2 of the GPL, the condition subsequent had occurred with the result that Defendant had lost its license.

In a second place, the Court also ruling on the objection of the defendant that the data storage units already sold by Defendant were covered by the principle of exhaustion of the right to distribute, noted that such exhaustion never took place, since they were not put into circulation by sale with the consent of the authors as the sale of the data storage units did not comply with the GPL. However, purchasers could, at any time, acquire the necessary rights of use (the three programs) directly from the author by recognising the GPL.

In the relevant judgement, one might extract that there would be some hypothetical possible ways that the GPL, as a whole contract itself, might have been declared invalid with the further result that defendant had never been a licensee and a copyright infringement by the Defendant took place at once. This might have happened if:

- a) the GPL were not sufficient to form a legal relationship with Plaintiff according to the rules governing the formulation of the contract
- b) due to antitrust provisions, Sec. 2 of the GPL was declared invalid and because of its inseparable connection to the primary obligation (the grant of the license) the whole contract was invalid pursuant to Section 139 of the German Civil Code (BGB)

---

48. In quite similar thoughts to those formulated in *Harald Welte v. S(itecom)*.

In all the above ways, plaintiff would also be entitled to plead invalidity of the entire contract and therefore allege that Defendant is lacking any license<sup>49</sup>.

### iii) Harald Welte v. Fortinet

For the sake of completeness we address two more cases brought by Welte before the German Courts. The first case concerned Fortinet UK Ltd., the UK subsidiary of Fortinet Inc., which used GPL software in certain products and then used cryptographic techniques to conceal that usage. In particular, Fortinet offered a variety of Firewall and Antivirus Products (the FortiGate and FortiWiFi product series), on which Fortinet claimed to run the “FortiOS” operating system. However, as the gpl-violations.org project uncovered, “FortiOS” was using the Linux operating system kernel and numerous other free software products that were licensed exclusively under the GNU GPL. This information was not disclosed by Fortinet.

Following a warning notice by the gpl-violations.org project on March 17, 2005, Fortinet did not sign a declaration to cease and desist. Out-of-court negotiations on a settlement failed to conclude in a timely manner. Thus, the gpl-violations.org project was compelled to ask the court for a preliminary injunction, banning Fortinet from distributing its products, unless they were in full compliance with the GNU GPL license conditions.

As a result of this violation, the Munich district court granted a preliminary injunction against Fortinet Ltd., banning it from further distribution of their products until they were in compliance with the GNU GPL conditions regarding the provision of the full corresponding source code and a copy of the full license text<sup>50</sup>.

### iv) Harald Welte v. Skype Technologies SA

The other noticeable case involving Harald Welte concerned the Luxembourg-based Skype Technologies SA, well known as an Internet telephony provider, engaging in the distribution of GPL software without simultaneously providing the source code royalty-free, and without attaching the text of the GPL (v. 2.0.) license. The source of the conflict was the fact that the SMCWSKP 100 VoIP phone made by SMC Networks was being offered for sale on the website of Skype Technologies SA (the respondent). According to the court’s findings of fact, the vendor of the VoIP telephone was a Spanish distribution enterprise, which used the website of the respondent for promoting its sales. The firmware of this VoIP tel-

---

49. That was also a matter considered similarly in *Harald Welte v. S(itecom)*.

50. We do not address the rationale of the Court, since that is fully based on the case-law established in Germany by Welte’s actions.

ephone used the Linux operating system, and it included two programs to which Harald Welte (the applicant) held exclusive rights. The two programs were free software, which may be used according to the terms of the GNU GPL version 2.0.

In the relevant case, also known as *Harald Welte v. Skype Technologies SA*<sup>51</sup>, the First Regional Court of Munich thought that, according to section 1 of the GNU GPL, the licensee may distribute the software only on condition that a copy of the license text is included. In selling the VoIP telephone at the root of this conflict, the text of the license was not included. Furthermore, this VoIP phone was being distributed contrary to the GNU GPL terms concerning the distribution of object code. Section 3 of the GNU GPL permits the distribution of object code, but only if the licensee fulfils certain conditions. The distribution of software as object code conforms to the GPL only if the complete machine readable source code (sic) is provided at the same time on a usual medium for data exchange, and if the general terms of the GPL concerning the distribution of GPL licensed software are being observed. The way this VoIP telephone was offered for sale did not conform to these requirements.

In particular, the court found that after the respondent had learned that the promotion of the VoIP telephone was in conflict with the GPL, he began selling it with a supplementary sheet. On this document it was noted that the VoIP phone contained software which was licensed under the GPL or LGPL. Further it drew attention to where on the Internet one could find *the text of the license* and the *source code*.

As to the condition of the GPL regarding the text of the license the Court noted that the way the software was offered for sale violated section 1 of the GNU GPL despite the inclusion of the supplementary sheet. This section of the GPL requires that the recipient of the program must also receive the text of the license. It is therefore insufficient to only offer him the possibility of retrieving it online. Finally, in the view of the court the reference to the applicability of the GPL and LGPL were too vague, particularly since the recipient of the program cannot distinguish, which of the two licenses is actually applicable. According to the court ruling, although the respondent was not the vendor of the telephone, after being made aware of the violation he was nonetheless obliged to investigate and to ensure that future sales of the VoIP telephone via his website was in conformance with the law.

The same were applicable as to the condition of the GPL of how to make available source code: the plaintiff was informed of the existence of this sheet only

---

51. Harald Welte v. Skype Technologies SA, (2007), First Regional Court of Munich, 7 O 5245/07.

when legal proceedings were underway. The court opined that the option of offering source code for download from the Internet is in the text of the GNU GPL (last paragraph of Section 3), but this applies only in the case that the object code is offered for download at the same location: “If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.” In all other cases, when selling software it is not sufficient to offer the source code only online.

The judgement in this conflict makes it unmistakably clear that an only approximate conformance to the GNU GPL is not sufficient, but also that violations of license details lead to the loss of rights for the license holder, and consequently make the use of GPLed software illegal. Put it otherwise, the judgement is of crucial importance since it accepts that the terms of the GNU GPL must be observed exactly, just like the clauses of every other contract. “Inaccuracies” in the observance of the license terms are violations of the law and make it illegal to use the software. The judgement also offers affirmation that the GNU GPL must be respected by persons resident outside Germany.

### **v) Educaffix28 v. CNRS**

The French Courts have also had the opportunity to address issues of validity and enforceability of F/OSS licensing terms. The first case ever in France (although of not significant importance in terms of our issue in question) was brought before the French Courts in 2007 by Educaffix28, a company that had concluded software transfer agreements with several higher education establishments and the CNRS. The transferred software could, however, only work with a free software, JATLite, developed by the University of Stanford under GNU GPL license. Educaffix requested that the contract be declared null and void for fraud on the basis that CNRS had concealed the fact that the existence of the free software included in the transfer agreement required permission from a third party holder of the rights over said free software, in this case the University of Stanford. Further, Educaffix requested that the contract be revoked for the sole fault of CNRS because the exploitation of the transferred software implied by necessity the commission of an act of piracy over the free software.

In the relevant case, well known as *Educaffix28 v. CNRS*<sup>52</sup>, The court held:

“this program has the particular feature of depending on a GNU license which allows free use of the software, but requires a license if the work based on the

---

52. *Educaffix28 v. CNRS*, (2007), no further citation information are known to the author.

program can not reasonably be identified as independent and must therefore be considered as a derivative of the JATLite program.”

This decision is understood by some commentators to constitute an application of the provisions of the GNU license and refers to, without directly citing, section 2 of the GNU license<sup>53</sup>, by virtue of which the judges recognize the contaminant nature of a derived program (Perbost and Walter, 2011).

It should be noted, however, that the decision does not explicitly recognize the validity of the GNU-GPL license, in as far as it would have been up to the holder of the rights (University of Stanford, or transferee) acting on the legal principle of piracy and requesting the recognition of its rights, which was not the case here.

#### **vi) Société EDU 4 v. AFPA**

Perhaps the most commented judgement of French Courts was that decided in *Société EDU 4 v. AFPA*<sup>54</sup>. In that case, the National Association for Adult Education (AFPA) issued a call to tender for the implementation of learning spaces, which was finally granted to EDU 4. Raising doubts about the sincerity of the offer submitted by EDU 4, AFPA declared the contract terminated. EDU4 felt that they had delivered in accordance, and sued AFPA for abusive breach of contract, a claim upheld by the High Court of Bobigny in 2004.

Before the Court of Appeal, AFPA claimed that EDU4 had not clearly informed them that free software had been incorporated into the solution provided, that copyright mentions linked to the software had been modified and that the text of the GNU-GPL license had been removed. The Court of Appeal of Paris upheld the claims made by AFPA and held that EDU4 had failed to respect the terms of the GNU license.

The court found that the presence of GPL software had never been hidden, because the contractual documents were clear on that point. The court of appeal nevertheless ruled that the client had been entitled to refuse payment, for three main reasons:

---

53. Section 2 of the GPL reads:

«...these requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it».

54. *Société EDU 4 v. AFPA*, (2009), Court of Appeal of Paris.

First, the delivered software to be taken into account was the software provided to the client at the date of the validation procedure, and not the «corrected» software, delivered three months later. No preliminary version had ever been mentioned in the contractual documentation.

Second, the violation of the GPL *exposed the client to a copyright infringement lawsuit*, and thus the vendor was in breach of contract.

Third, the security loophole made the software unacceptable, and therefore legitimates the termination of the contract for a breach of its obligations by the vendor.

Some commentators argue that French court's language recognizes that GPL license is a valid license by –inter alia - acknowledging that the violation of the terms of the GPL could expose to a copyright lawsuit. It is seen as a standard application of French property laws regarding ejectment, since, pursuant to Article 1626 of the French Civil Code, the seller of a good ought to, inter alia, warrant its purchaser against any third party claim (Lamon, 2010). The core issue is not the license of GPL from the first author of a software to a company which uses it directly, but the sublicense of a GPL software from a licensee company to one of its clients. It is further argued that - with this decision - there is no further doubt that, while concluding the second license, the licensee company shall strictly abide by the terms and conditions of the first GPL (Perbost and Walter, 2011). However, this case was not an IPR case and - as such - no one could reasonably argue that the decision incorporates thoughts about the enforceability of the GPL, but rather an acknowledgment that the GPL is a valid contract (Willebrand, 2009). Anyway, we quote a part of the judgement which is relevant hereto:

“...(The court) considers that it follows from all of these elements that the entity EDU 4 had not fulfilled its contractual obligations with its delivery in December 2001, the date on which the performance of EDU 4 was to be assessed, that on the one hand posed privacy risks to the users of EOF and on the other hand did not satisfy the terms of the GNU GPL license, since the entity EDU 4 had removed the original copyright notices of VNC from two files, replacing them with its own copyright notices, and since it had deleted the text of the license;”

This decision is also important because it was feared that France, one of the countries with the highest levels of copyright protection, would deem the free license to be null and void (Perbost and Walter, 2011). Nevertheless, French Courts will have further opportunities in the future to address the issue of enforceability in terms of copyright law in a greater detail. The pending case of *Iliad*, filed in 2008, concerning the distribution of “Freebox” (the modem provided by the ISP “Free” to its customers) which is a software containing free software components, in

breach of the terms of the associated GPL license, might be seen as a unique opportunity towards this direction.

### **3. Reviewing the Global case-law**

As follows from the previous part, it seems that a remarkable body of case law has begun to expand in our decade globally and addresses the issues of validity and enforceability of F/OSS licensing terms and conditions. Given the fact that GNU GPL is by far the most prominent free license used in open source projects it is reasonable that most cases before the Courts concern this particular license. In this final part, we address segmental legal issues that have been raised by virtue of the existing – at the time of writing – case law and we hope to reach to useful conclusions thereto.

#### ***3.1. The validity and enforceability of a F/OSS license***

##### **3.1.1. The US approach**

In most common law jurisdictions (including USA) the legal nature of a F/OSS license is much debated on whether such agreement constitutes a license or a contract. (Gonzalez, 2009). In the USA, two competing theories attempt to explain why F/OSS licenses are enforceable. The first theory declares that such licenses are non contractual licenses rather than contracts. The second theory holds that they are contracts with offer, acceptance, consideration and a meeting of minds. This theory is plausible since traditional software licenses are generally regarded as contracts. But such licenses also have cash consideration. Contract proponents argue that consideration does not exist under the F/OSS licenses (in particular the GPL). But ultimately they are unable to show that there is a meeting of minds between the licensor and licensee, thus failing the requirements of contract formation (Wacha, 2005, Kumar, 2006). Anyway, the distinction is useful, since it differentiates the legal remedies to which licensor is entitled. So, if the terms of the F/OSS license allegedly violated serve as both contractual covenants and conditions, they may serve to limit the scope of the license and are governed by US Federal copyright laws. If they are merely covenants, by contrast, they are governed by State contract laws. To identify further whether a term within such a license is a condition or a covenant, a proper interpretation has to take place (Frazer, 2009). That has been a core issue addressed in American case law by virtue of the decision in *Jacobsen v. Katzer*. The Court of Appeals accepted that due to a relevant interpretation (linguistic and teleological) the attribution and reference requirements set forth by the Artistic license serve as conditions, under which the software is licensed. The Artistic license was treated as a license (in principle), but the Court did not clearly



settle the debate as to whether these licenses are also contracts, although there is much in the judgement to suggest this is the case (Fitzerald, Olwan, 2009). One could probably argue that *Jacobsen v. Katzer* decision regards F/OSS licenses not to lack consideration and that they, furthermore, meet the standards required by the modern contract law to form an enforceable contract. Some commentators argue that it is left unanswered of what a clearer definition about a covenant and a condition in American law consists. However, the phrase “provided that” within F/OSS licenses (the Artistic License and the GPL) is likely to constitute *conditions* of a license and not mere covenants in future litigation (Azzi, 2010). In any case, *Jacobsen v. Katzer* suggests that contracting parties to a license may craft license conditions as they fit, but calls on courts to vigorously enforce the boundaries, that already hem in license contracts and to exercise prudence in granting injunctions when license conditions scarcely touch on exclusive copyrights or serve the underlying goals of copyright (Gomulkiewicz, 2009).

### 3.1.2 The EU approach

At the same time, the relevant license/contract debate is not of *particular interest* in the legal traditions of Continental Europe as it is in common law jurisdictions. European Countries could probably treat F/OSS licenses as “contracts” incorporating the copyright licensing terms (Gonzalez, 2009). Since F/OSS licenses are pre-formulated and not individually negotiated between the parties, they may be regarded as general terms and conditions. In principle, the validity of those terms is essential for any kind of contract, but the underlying legal relationship between the parties concerned (B2B) or (B2C) plays an important role, since B2C contracts are subject to stricter rules, because the consumer is considered to be the weak party and therefore deserves higher protection (Legal IST Report, 2005). To that end, the applicability of Council Directive 93/13/EEC on unfair terms in consumer contracts (as incorporated in the national legislation of each single Member-State) harmonizing the consumer Contract law across the EU Member States depends largely on whether the contracting parties qualify as “seller/supplier” and “consumer” within the meaning of the Directive (Gonzalez, 2004).

However, many European jurisdictions provide for the applicability of the rules of general terms and conditions to any contract irrespective of the qualification of the party invoking these terms. This is particularly so with the German Civil Code (305-310). Moreover, the licensing terms should be specifically incorporated into the contract. Of the applicable rules one could arguably identify those included in the “E-Commerce” Directive<sup>55</sup>, which is applicable both in B2B and in B2C.

---

55. Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the internal market.

As already noted, in *Harald Welte v. D-Link* the German Court considered the license conditions as general conditions of sale that are to be checked according to par. 305 ff. BGB, which contain the German consumer protection law dealing with standard terms of business. In the case of free software it is to be assumed that the copyright holder by putting the program under the GPL makes an offer to a determinable or definite circle of people and that this offer is accepted by users (of the software) through an act that requires consent under copyright law; in this respect, it can be assumed that the copyright holder enters into this legal relationship without receiving an actual declaration of acceptance according to Section 151 of the German Civil Code (BGB). The conditions of the license granted under the GPL must be regarded as standard terms and conditions that are subject to Sections 305 et seq. of the German Civil Code (BGB). Since the conditions of the license granted by the GPL are easily available on the Internet, they were without a doubt incorporated into the contractual relationship between the authors and Defendant (Section 305, Subsection 2, No.2 of the German Civil Code (BGB)).

Such judicial approach, followed by the entirety of the German and French<sup>56</sup> case law, reflects the prevailing opinion of legal scholars that all questions related to the validity and enforceability of the GPL will be dealt with using the same German legal norms applied to any standard terms of business and seems compatible to the applicable legal framework above (Hoppner, 2004).

### ***3.2. The validity and enforceability of F/OSS licensing terms – common understandings***

We have already noted above, which terms within the relevant F/OSS licenses have been declared valid and enforceable before the Courts globally: the attribution and reference conditions of the Artistic Licence in *Jacobsen v. Katzer* and sections 2, 3 and 4 of the GPL (v.2) by the German Courts. Even more, in the precedent case *Harald Welte v. Sitecom*, the Court also held that the incorporation of the GPL in English language was held valid, because the contract in question had been concluded between business persons. Finally, the French Courts have not analyzed the issue of enforceability of the GPL in considerable depth, but seem to treat such a license as a contractual agreement in line with the existing legal framework. At this point, however, what seems to be of crucial importance is to extract some useful findings with regard to the common underlying principles by which the global Jurisprudence is driven.

---

56. Although not explicitly.

### 3.2.1. F/OSS licenses as broad licenses

Software distributed to the public under an open source or copyleft licensing regime is often said to be in the public domain. This is not accurate, since the decision to license the use of one's works under a copyleft licensing scheme does not amount to a relinquishment of copyright but rather as exercise thereof, albeit different. In the field of copyright law, a copyleft strategy enables creating a sphere of free use without giving up the exclusivity one owns in the intellectual creation. It is totally irrelevant that such licensing may pursue objectives similar to those of the public domain (free availability, use and exploitation of creative expressions) (Dusollier WIPO, 2010).

Moreover, the freedom of use afforded under most F/OSS licenses does not, as such entail a waiver of right on the part of the copyright holder. On the contrary, the grant of a permission to execute certain acts with respect to copyright protected software falls within the scope of the copyright holder's exclusive rights and must be distinguished from a waiver of right. If the licensor waived his exclusive rights with regard to the software, there would be logically no consequence attached to the non-respect of the conditions by the licensee (Guibault, 2006). Instead, many F/OSS licensing terms (e.g. in GPL or MPL) provide for the termination of the license, if licensee does not abide by the very specific terms of the license, thereby placing the latter in the legal position of acting without a respective right and thus infringing copyright. This is exactly the peculiar way that "copyright infringement" is conceptualized in a F/OSS licensing scheme. Thus, instead of regarding software distributed under such a licensing regime as left to the public domain or regarding such licenses as entailing a waiver of right on part of the copyright holder, it would be advisable to understand those licenses as involving a broad permission, the validness of which depends largely on the consistent observance on behalf of the licensee. Once the latter violates the terms of such license (the GPL for instance), the agreement terminates and a copyright infringement occurs.

The global vase law supports this finding. The language of German Court's rulings in *Harald Welte v. S(itecom) Deutschland GmbH*, *Harald Welte v. D-Link* and *Harald Welte v. Skype* seems to conceptualize GPL as a means for an author to exercise his exclusive rights under copyright, by establishing the conditions under which a piece of software may be legally copied, modified and further distributed and, therefore, sharing the view of the "broad" character of the license permission:

"...The Court shares the opinion that the conditions GPL (General Public Lizen(s)e) cannot be considered a waiver of copyright and authorship rights.

To the contrary, conditions of copyright law serve the users to ensure and realize their goals regarding further development and distribution of software”<sup>57</sup>.

“...the conditions of the GPL can in no case be interpreted to contain a waiver of legal positions afforded by copyright law. The GPL precisely stipulates that the freedom to use, modify and distribute the corresponding software initially afforded by way of a grant of a non-exclusive license to everyone is automatically terminated upon a violation of the GPL (citation omitted)”<sup>58</sup>.

The language used by the German Courts at this point is quite similar to that used by the US Courts in *Planetary Motion, Inc. v. Techplosion, Inc.* and the subsequent American case law:

“...Appellants misconstrue the function of a GNU General Public License. Software distributed pursuant to such a license is not necessarily ceded to the public domain and the licensor purports to retain ownership rights, which may or may not include rights to a mark”<sup>59</sup>.

“...The court’s understanding from the GPL itself is that it is a software licensing agreement through which the GNU/Linux operating system may be licensed and distributed to individual users so long as those users ... (section 3 GPL). ...the GPL ...merely acts as a means by which certain software may be copied, modified and redistributed without violating the software’s copyright protection”<sup>60</sup>.

“Authors, who distribute their works under this license, devised by the Free Software Foundation, Inc., authorize not only copying but also the creation of derivative works -- and the license prohibits charging for the derivative work. People may make and distribute derivative works, if and only if they come under the same license terms as the original work. ...Neither the original author, nor any creator of a revised or improved version, may charge for the software or allow any successor to charge. Copyright law, usually the basis of limiting reproduction in order to collect a fee, ensures that open-source software remains free: any attempt to sell a derivative work will violate the copyright laws, even if the improver has not accepted the GPL. The Free Software Foundation calls the result “copyleft””<sup>61</sup>.

---

57. *Harald Welte v. S(itecom) Deutschland GmbH*.

58. *Harald Welte v. D-Link*.

59. *Planetary Motion, Inc. v. Techplosion, Inc.*

60. *Daniel Wallace v. Free Software Foundation, Inc.*

61. *Daniel Wallace v. International Business Machines Corporation, Red Hat, Inc. and Novell, Inc.*

“...In this case, a user...is authorized to make modifications and to distribute the materials “provided that” the user follows the restrictive terms of the Artistic License. ...Copyright holders who engage in open source licensing have the right to control the modification and distribution of copyrighted material...A copyright holder can grant the right to make certain modifications, yet retain his right to prevent other modifications. Indeed, such a goal is exactly the purpose of adding conditions to a license grant. The Artistic License, like many other common copyright licenses, requires that any copies that are distributed contain the copyright notices and the COPYING file...The clear language of the Artistic License creates conditions to protect the economic rights at issue in the granting of a public license. These conditions govern the rights to modify and distribute the computer programs...”<sup>62</sup>.

It seems more than just clear that all Courts share the view that it is at the will of the copyright holder to adopt a F/OSS license as the sole licensing mechanism of the copyrighted work and could refuse to allow copying, modification or distribution under any other terms (Carver, 2005). The German case law has made it absolutely clear that since the copyright holder chooses such form of licensing, *an only approximate conformance to the License is not sufficient*, but also that *violations of license details lead to the loss of rights* for the license holder:

“If a publisher wants to publish a book of an author that wants his book only to be published in a green envelope, then that might seem odd to you, but still you will have to do it as long as you want to publish the book and have no other agreement in place”<sup>63</sup>.

### 3.2.2. The goal of F/OSS projects as protected by law

Notwithstanding, similar common understandings may be found in the global case law that endeavors by F/OSS proponents to achieve the greatest level of software development in favor of the F/OSS community *is a concept understandable and protectable by the law itself*. If courts refused to uphold the validity of a F/OSS license, the consequences for the open source community, which relies on such a license for the continuity of its development practices could be devastating. The strength of the GPL and other open source licenses lies precisely in their moral force. The language of the Courts is, herein, undoubtedly persuasive:

“...The GPL purportedly functions to “guarantee (users’) freedom to share and change free software.” (GPL Preamble.) As alleged, the GPL in no way forecloses other operating systems from entering the market...the GPL encourag-

---

62. *Jacobsen v. Katzer*.

63. *Harald Welte v. Skype* (paraphrasing from Welte).

es, rather than discourages, free competition and the distribution of computer operating systems, the benefits of which directly pass to consumers”<sup>64</sup>.

“Thus, the GPL propagates from user to user and revision to revision: neither the original author, nor any creator of a revised or improved version, may charge for the software or allow any successor to charge. Copyright law, usually the basis of limiting reproduction in order to collect a fee, ensures that open-source software remains free: any attempt to sell a derivative work will violate the copyright laws, even if the improver has not accepted the GPL. The Free Software Foundation calls the result “copyleft””<sup>65</sup>.

“...Through such collaboration, software programs can often be written and debugged faster and at lower cost than if the copyright holder were required to do all of the work independently...” Copyright licenses are designed to support the right to exclude; money damages alone do not support or enforce that right. The choice to exact consideration in the form of compliance with the open source requirements of disclosure and explanation of changes, rather than as a dollar-denominated fee, is entitled to no less legal recognition. Indeed, because a calculation of damages is inherently speculative, these types of license restrictions might well be rendered meaningless absent the ability to enforce through injunctive relief...The attribution and modification transparency requirements directly serve to drive traffic to the open source incubation page and to inform downstream users of the project, which is a significant economic goal of the copyright holder that the law will enforce...”<sup>66</sup>.

“...the legislator expressly recognizes the fundamental principle of open source software with the provision in par. 32 section 3 sentence 3 UrhG”<sup>67</sup>.

### 3.3. Conclusive remarks

To address all the legal issues that may arise in the context of validity and enforceability of F/OSS licensing terms would probably be a subject matter of a book and not of a mere contribution of a particular length. In this paper, the author attempted to cite all the relevant case law that exist - to his knowledge - at of the date of writing. Many and serious questions have remained unanswered: from an American law perspective the landmark rule in *Jacobsen v. Katzer* has raised issues that enhance the license/contract debate by not drawing a clear line in the definitions between “conditions” or “contractual covenants” of a license.

---

64. *Daniel Wallace v. Free Software Foundation, Inc.*

65. *Daniel Wallace v. International Business Machines Corporation, Red Hat, Inc. and Novell, Inc.*

66. *Jacobsen v. Katzer*.

67. *Harald Welte v. Sitecom*.

At the same time many issues within the GPL that have not been analysed by the European Courts in the light of the existing European framework; some of them might include e.g. the question of the applicable law, the use of general conditions in a foreign language, the automatic termination clause in case of breach of some obligations under the contract, the copyleft provision etc (Hoeren, 2004).

Despite the technical details that constitute the factual context of each single case and whereas copyright laws from different States and legal traditions are involved, it is not exaggeration to say that still judges from America, Germany and France share some common understandings. These understandings, as outlined above, may extend from the crucial consideration of intellectual property that a copyright holder retains the exclusive rights in a F/OSS licensing scheme by creating conditions to which licensees must adhere, to the most important legal recognition of the goal that F/OSS community pursues in such context.

All these considerations leave no doubt that judges do remain aware of global trends in Intellectual Property Law (O'Neil and Gaspar, 2010). The pioneering body of case law developed by the German Courts - in particular - created a de facto precedent for American Courts in Information Technology Law and policy. What needs to be seen is whether open source as an alternative model of traditional proprietary software will achieve its primary goal to deliver the global community the benefits of innovation at the lowest possible cost. As long as this remains true, the global jurisprudence informs us that this is "...a significant economic goal ... that the law will enforce...".

## References

- Armstrong T., (2010), "*Shrinking the commons: termination of copyright licenses and transfers for the benefit of the public*", Harvard Journal on Legislation, vol. 47, 376.
- Azzi M., (2010), *CPR: how Jacobsen v. Katzer Resuscitated the open source Movement*, University of Illinois Law Review, vol. 2010, 271.
- Briggs P., (December 31, 1969-January. 7, 1970), "IBM unbundling biggest software event in 1969," Computerworld, volume 4, p.15.
- Brown C., (2010), *Copyleft, the disguised copyright, why legislative copyright reform is superior to copyleft licenses*, 78 UMKC, L. REV. 749, pp. 761-763.
- Buchanan O'Neil J. & Gaspar C., (2010), "*What can decisions by European Courts teach us about the future of the open source litigation in the united States*", AIPLA Quarterly Journal, vol. 38, no. 4, 437.

Buning M., (2007), "The history of copyright protection of computer software: The emancipation of a work of technology toward a work of authorship" in "The History of Information Security", a Comprehensive Handbook.

Carver B., (2005), "*Share and share alike: understanding and enforcing open source and free software licenses*", Berkeley Technology Law Journal, vol. 20, 469.

Dusollier S., WIPO, (2010), "*Scoping study on copyright and related rights and the public domain*", CPID/4/3REV/STUDY/INF./1.

Fitzerald B. and Olwan R. (2009), *The legality of free/open software licenses: The case of Jacobsen v. Katzer*", Journal of Sharia and Law, No. 40.

Frazer B., (2009), *Open source is not public domain: evolving licensing philosophies*, Idaho Law Review, vol. 45, 349.

Gatto J., (2007), *Doubts wane over GPL enforceability, managing intellectual property*, online at <<http://www.pillsburylaw.com/siteFiles/Publications/A9A22185D029BBE6EAA4332F1A7249E2.pdf>>, accessed 26.03.2011.

Gomulkiewicz R., (2007) "A first look at General Public License 3.0, The Computer and Internet Lawyer", vol. 24, no. 11.

Gomulkiewicz R., (2009), "*Conditions and covenants in license contracts, testing from a test of the artistic License*", Texas Intellectual Property Law Journal, vol. 17, no. 3.

Groklaw, (2007), "*Judge Kimball administratively closes SCO v. IBM pending bankruptcy proceedings of SCO*", online at: <<http://groklaw.net/article.php?story=2007092110013091>>, accessed 26.03.2011.

Guatamuz Gonzalez A., (2004), *Viral contracts or unenforceable documents?: contractual validity of copyleft licenses*, E.I.P.R., 335.

Guatamuz Gonzalez A., (2006), "*GNU General Public License v.3: a legal analysis*", Script-Ed, Vol. 3, Issue 2.

Guatamuz Gonzalez A., (2009), "*The license/contract dichotomy in open licenses: a comparative analysis*", University of La Verne Law Review, Vol. 30, no. 2, 296.

Guibault L., (2006), "*Paradigm shift in European intellectual property law? from Microsoft to Linux*", Lex Electronica, vol. 10, no. 3.

Hass D., "*The Gentlemen's Agreement Soldiers On, Linux under GNU, General Public Licenses 2 and 3*", online at: <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1330020](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1330020)>, last accessed 26.03.2011.



Hoeren T., (2004), "*The first ever ruling on the legal validity of the GPL: a critique of the case*", online at: <[http://www.oii.ox.ac.uk/resources/feedback/OIIFB\\_GPL3\\_20040903.pdf](http://www.oii.ox.ac.uk/resources/feedback/OIIFB_GPL3_20040903.pdf)>, accessed 26.03.2011.

Hoppner J., (2004), "*The GPL prevails: an analysis of the first-ever court decision on the validity and effectivity of the GPL*", Script-ed, vol.1, no. 4.

Kumar S., (2006), *Enforcing the GNU GPL*, Journal of Law, Technology and Policy, No.1, pp. 1-36.

Lamon B., (2010), *Validity of GPL License*, Computer Law Review International CRI.

Lee S., (2010), "*Open source software licensing*", online at: <<http://cyber.law.harvard.edu/openlaw/gpl.pdf>>, last accessed 26.03.2011.

Legal IST, (2005), *Report on legal issues in open source software*.

Madison M., (2004), *Reconstructing the software license*, Loyola University Chicago Law Journal, vol. 35, p. 280.

Martin W., (2009), "*A look at EDU 4 v. AFPA, also known as the "Paris GPL case"*", IFOSS L. Rev., 1(2), . 123 – 126.

Perbost F. and Walter A. (Kahn & Associés), (2011), *The International Free and Open Source Software Law Book*, France.

Reidenberg J., (2007), *The rule of intellectual property law in the Internet economy*, Houston Law Review, vol. 44:4, 1091.

Software Freedom Law Center, (2008), *A legal issues primer for open source and free software projects*, online at: <<http://www.softwarefreedom.org/resources/2008/foss-primer.html#fn2x4-bk>>, last accessed 26.03.2011.

St. Laurent A., "*Understanding open source and free software licensing*", online at: <<http://oreilly.com/catalog/osfreesoft/book/>>, last accessed 26.03.2012.

Szinger A., (2001), *Copyright protection of software, colloquium on language diversity in Information society*, online at: <<http://www.ajk.elte.hu/TudomanyosProfil/kiadvanyok/elektronikus/akademia/SzingerAndras-LegalRules.pdf>>, accessed 26.03.2012.

Wacha J., (2005), "*Taking the Case: Is the GPL Enforceable?*", Santa Clara Computer and High Tech. L. Journal, vol. 21, 453.

Wikia, (2011), "*IBM unbundling of software and services*", online at: <<http://itlaw.wikia.com/wiki/Unbundling>>, last accessed 26.03.2012.

WIPO (2011), "*Technological and legal developments in Intellectual property*, in *WIPO Intellectual Property Handbook: Policy, Law and Use*", p. 436.

WIPO, (2011), *Basic notions of copyright and related rights*, online at <[http://www.wipo.int/export/sites/www/copyright/en/activities/pdf/basic\\_notions.pdf](http://www.wipo.int/export/sites/www/copyright/en/activities/pdf/basic_notions.pdf)>, accessed 26.03.2011.

WIPO, (2011), *Introduction to the WIPO Copyright Treaty*, online at <<http://www.wipo.int>>, accessed 26.03.2011.

### **Case Law**

*Daniel Wallace v. Free Software Foundation, Inc.*, (2005), U.S. District Court, Southern District of Indiana, Indianapolis Division, 31728, 7 - 8.

*Daniel Wallace v. International Business Machines Corporation, Red Hat, Inc. and Novell, Inc.*, (2006), Court of Appeals for the 7<sup>th</sup> Circuit, 467 F.3d 1104.

*Educaffix28 v. CNRS*, (2007).

*Harald Welte v. D-Link*, (2006), District Court of Frankfurt am Main 2-6 0 224/06.

*Harald Welte v. S(itecom) Deutschland GmbH*, (2004) District Court München I file number: 21 O 6123/04.

*Harald Welte v. Skype Technologies SA*, (2007), First Regional Court of Munich, 7 O 5245/07.

*Planetary Motion, Inc. v. Techplosion Inc.*, (2001), Court Of Appeals For The 11th Circuit, 261 F.3d 1188.

*Robert Jacobsen v. Matthew Katzer and Kamind Associates*, (2007), U.S. Dist. LEXIS 63568, 2007 WL 2358628.

*Robert Jacobsen v. Matthew Katzer and Kamind Associates, Inc.*, (2008), Court of Appeals for the Federal Circuit, 535 F.3d 1373.

*S.O.S., Inc. v. Payday, Inc.*, (1989) 9<sup>th</sup> Circuit, 886 F.2d 1081, 1087; *Nimmer on Copyright*, § 1015(A) (1999).

*SCO Group, Inc. V. IBM*, Civil action No 2:03cv0294.

*SCO Group, Inc. v. Novell*, Civil Action No 2:04cv139.

*SCO Group, Inc. v. Novell, Inc.* (2009), Court of Appeals for the 10<sup>th</sup> Circuit, No. 08-4217.

*Société EDU 4 v. AFPA*, (2009), Court of Appeal of Paris.

*Sun Microsystems, Inc., v. Microsoft Corp.*, (1999), 9<sup>th</sup> Circuit, 188 F.3d 1115, 1121; *Graham v. James*, 2<sup>nd</sup> Circuit, 144 F.3d 229, 236.

# Law and ethics in the modern EU 'surveillance society': are data protection principles 'dead' in the area of freedom, security and justice?

## The case of VIS and EURODAC information systems

---

---

Maria Tzanou

---

---

*"The problem with databases emerges from subjecting personal information to the bureaucratic process with little intelligent control or limitation, resulting in a lack of meaningful participation in decisions about our information."*<sup>1</sup>

### I. Introduction

Database has been eloquently described as 'the biggest change brought about by the information technology revolution'.<sup>2</sup> Indeed, multiple data can now be gathered, processed, tabulated and cross-referenced at speeds and with accuracy that would have been unthinkable in the past. In today's information society, where the collection, storage, use, collation and communication of vast amounts of personal data are central to the functioning of public services as well as private business, computer databases and computer networks are becoming almost ubiquitous.<sup>3</sup>

It goes without saying that databases are crucial for law enforcement. The storage and exchange of information through large-scale databases that interlink to each other is a very powerful apparatus for law enforcement authorities, in particular in the fight against terrorism. For this reason, a proliferation of cross-border information systems used for law enforcement purposes has been witnessed

- 
1. Daniel Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy", 53 *Stan. L. Rev.* (2001), 1393, 1422. On the great variety of databases see Bottis M., *The legal protection of databases*, 2004, Nomiki Bibliothiki, in Greek.
  2. 'A report on the surveillance society: For the Information Commissioner by the Surveillance Studies network', September 2006, available at [http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/surveillance\\_society\\_full\\_report\\_2006.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf), para 9.6.1.
  3. Surveillance society report, above n 1, para 9.6.1.

over the past few years. This 'security web'<sup>4</sup> is currently being spun at national, supranational and transatlantic levels alike.

However, despite the obvious benefits, large-scale databases raise many questions. What information is stored in them and for how long? How 'secure' are they? Who accesses them? Is there any accountability for the processors of personal information stored in databases? But above all: what are their implications on the rights to privacy and data protection of the individuals? What rights has the individual to check and, if necessary, to correct data held about himself or herself?

Writing on computer databases, Daniel Solove argued that the Big Brother metaphor, that is often used by journalists, politicians, jurists, and legal academics to describe the privacy problem created by the collection and use of personal information through databases is the wrong paradigm, and the metaphor of Franz Kafka's *The Trial* should be used instead as because it depicts in the correct terms the problems posed by databases to data privacy.<sup>5</sup> According to Professor Solove, the problems caused by the collection and storage of information in databases should not be couched on terms of surveillance, because databases do not 'uncover one's hidden world', nor do they 'disclose concealed information'. On the contrary, the problem posed by databases "is the powerlessness, vulnerability, and dehumanization created by the assembly of dossiers of personal information where individuals lack any meaningful form of participation in the collection and use of their information."<sup>6</sup> While Professor Solove makes a strong point, I will all the same use the Big Brother paradigm for the present discussion. There are two reasons for that: first, the 'surveillance paradigm' does not ascribe to the databases that will be examined, but to the EU instead. In this context, I will explain why I consider the EU as an 'emerging surveillance society'. Secondly, and more importantly, I will argue that specifically in the law enforcement context, the Big Brother metaphor seems the most appropriate one.

The paper will proceed as follows: first, I will attempt to sketch out why the European Union (EU) can be considered as an emerging surveillance society and what implications this has on the right to personal data protection as protected within this legal order. I will start by defining the surveillance state or the surveillance society and by identifying its main characteristics (II). I will then exam-

---

4. F. Geyer, *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice* [2008] <[http://shop.ceps.eu/BookDetail.php?item\\_id=1650](http://shop.ceps.eu/BookDetail.php?item_id=1650)> Centre for European Policy Studies, Research paper No. 9, retrieved 10 May 2011, 2.

5. Daniel Solove, above n.1, 1420.

6. Daniel Solove, above n.1, 1420.

ine to what extent the characteristics of the surveillance society can be applied to the EU (III). Subsequently, I will discuss the dangers posed to the right to data protection by the EU as an emerging surveillance society. For this reason, I will focus, in particular, on two case studies that pose the particular problem of ‘function creep’: the Visa Information System (VIS) database and EURODAC (IV). I will conclude with a critical note on the risks posed to fundamental rights and the rule of law when the EU is acting as a surveillance society (V).

## II. Defining the ‘Surveillance society’

In academic literature, the term “Surveillance society” has been used in a plethora of political science studies<sup>7</sup> already since the 1980s<sup>8</sup> in order to describe a computer-based society where information plays a crucial role within the bureaucratic control exercised by the national state.

Be that as it may, the notion of ‘surveillance society’ does not fit well in the legal discipline, as it is far from being a legal notion itself. Problems of definition in a legal text of a non-legal concept hence arise. However, I will use the term ‘surveillance society’ merely *instrumentally*,<sup>9</sup> insofar as it is needed in order to demonstrate my main thesis which views regards the privacy-intrusive measures adopted by the EU within the general context of the fight against terrorism.

In an article (2006) 2006, Balkin and Levinson note that the ‘National Surveillance State is characterized by a significant increase in government investments in technology and government bureaucracies devoted to promoting domestic security and (as its name implies) gathering intelligence and surveillance using all of the devices that the digital revolution allows.’<sup>10</sup> We can discern three parts in this definition: the first one concerns the increased engagement of the National Surveillance State in intelligence gathering and surveillance activities; the second regards the use of new technologies and technological devices to facilitate this process; finally, the third deals with the overall goal of the surveillance activities which is the safeguarding and promotion of national security.

For the purposes of the present analysis, the aforementioned definition will be adopted. I need to clarify of this point that I will not refer to the “National Surveillance State” but only to the “Surveillance Society”.

7. Surveillance society report, above n 1, para 3.5 and references therein.

8. The first reference to surveillance society was made by Gary T. Marx in 1985.

9. Emphasis added.

10. Balkin, Levinson, J. Balkin and S. Levinson, ‘The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State’, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=930514](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=930514), p. 131.

### III. The EU as an emerging 'Surveillance society'

The main thesis of the paper present contribution is that the European Union (EU) is acting after the 9/11 terrorist attacks and especially after the Madrid and London bombings, as an emerging 'Surveillance Society'. In particular, I argue that one can identify, with a number of *caveats* that will be analyzed later, the basic characteristics of the surveillance society in the EU. This assumption is based on the emphasis that the European Union has placed over the past years on the creation of an extensive toolbox for the collection, storage, and exchange of information between national authorities and other European players in the area of freedom, security, and justice.

As seen above, the surveillance society is characterized by 1) an increased engagement in intelligence gathering and surveillance activities 2) the use of new technologies and technological devices and 3) the overall goal of enhancing security. As will be demonstrated below, these characteristics can be found in the EU's actions and policies after 9/11. However, a further clarification is needed here. The surveillance-related activities of the EU are mainly pinned down in the exchange of information through large-scale centralised databases in the Area of Freedom, Security, and Justice (AFSJ). Below, the main characteristics of the EU's surveillance society-related policies, i.e 'information exchange' for the safeguarding of security, are set out.

#### *i. The New Age of Information exchange: from the Hague to the Stockholm Programme vision*

Facilitating the exchange of and access to information for the fight against terrorism, but also more generally to ensure security, has been high on the political agenda of the European institutions over the past few years.<sup>11</sup> This is because the exchange of data is becoming more and more essential for law enforcement in 'high profile' fields, such as counter terrorism. In its Communication of 10 June 2009 on an area of freedom, security and justice serving the citizen, the Commission notes that 'security in the EU depends on effective mechanisms for exchanging information between national authorities and other European players. To achieve this, the EU must develop a "European Information model" based on a more powerful strategic analysis capacity and better gathering and processing of operational information.'<sup>12</sup>

---

11. Hijmas and Scirocco, 'Shortcomings in EU Data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?', 2009 CMLR 46, 1485, 1489.

12. COM2009 (262) final, p. 16.

Against this background, the exchange of personal data between the law enforcement authorities in the different Member States has become lately a common scenario in the area of Freedom, Security and Justice. In this regard, improving the exchange of information was one of the central elements of the 'Hague Programme', the EU's five year Action Plan for Freedom, Justice and Security, purported to be (2005-2010) adopted on 5 November 2004 by the European Council in response to the 'war on terrorism'.<sup>13</sup> Under the headline 'Strengthening Security', the 'Hague Programme' included the so-called 'principle of availability', which purported the governing standard for information flows throughout the Union. According to this principle, 'a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State'. This means that full use of new technologies should be made in order to establish reciprocal access to national databases, interoperability as well as direct (online) access to existing central EU databases.<sup>14</sup>

Currently, a number of EU databases and systems of information exchange are already in place, while others are envisaged to become operational soon. However, as a scholar notes eloquently, it appears as if the EU is only at the beginning of a 'new age of information exchange'.<sup>15</sup> The EU's information exchange architecture in the area of Freedom, Security and Justice involves various different actors and is conducted for a number of different purposes. In particular, four actors can be identified: the EU, its Member States, private parties, and third countries (or international organisations). This leads to four different exchange possibilities: first, there is the possibility of reciprocal data transfers between Member States and EU institutions in the framework of centralized databases. These are namely the databases of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS) that store data input by

---

13. The Hague Programme: strengthening freedom, security and justice in the European Union, OJ C 53, 3.3.2005, p. 1.

14. See Statewatch analysis of the 'principle of availability', available at <<http://www.statewatch.org/analyses/no-59-p-of-a-art.pdf>>, according to which 'the "principle of availability" and data protection... are absolutely irreconcilable... The principle of availability and the "free market" in access to all (present and future) national or EU databases is a classic example of how EU governments have used the "war on terrorism" to give the emerging EU state sweeping powers of surveillance and control'.

15. F. Geyer, *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice* [2008] <[http://shop.ceps.eu/BookDetail.php?item\\_id=1650](http://shop.ceps.eu/BookDetail.php?item_id=1650)> Centre for European Policy Studies, Research paper No. 9, retrieved 10 May 2011.

the Member States, and provide access to them for law enforcement purposes.<sup>16</sup> The second possibility is the exchange of information between Member States and private actors (public/private partnership in combating crime). An example of this is the draft Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes.<sup>17</sup> This obliges air carriers to make the PNR data of passengers on international flights available to competent authorities for the purpose of preventing and combating terrorist offences and organized crime.<sup>18</sup> A third option is the data transfer between private actors and third countries. Under this category falls, for instance, the transmission of PNR data to the US, or the SWIFT case.<sup>19</sup> Finally, the fourth possibility is the exchange of data between Member States themselves, based on intergovernmental agreements, such as the Prüm Treaty regulating enhanced cross-border cooperation, particularly in combating terrorism and cross-border crime, which was signed in May 2005 by seven EU Member States.<sup>20</sup>

The 'Stockholm Programme', which is the next EU's five year plan for Justice and Home Affairs (2010-2014), endorses an even more powerful vision of surveillance society elements. In particular, it sets out a number of policies to be adopted and implemented in the area of freedom, security and justice that demonstrate quite clearly that the EU's surveillance-related aspirations are even more serious than before. In the Programme, the European Council calls for a definition of a comprehensive EU internal security strategy based, *inter alia*, on a proactive and intelligence-led approach, that requires stringent cooperation between EU agencies, including a further improvement of their information exchange.<sup>21</sup>

According to the Programme, security in the EU requires an integrated approach in which security professionals share a common culture, pool information as effectively as possible and have the right technological infrastructure to support

---

16. Geyer, above n 15.

17. Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, COM (2007) 654.

18. Another example of the public/private partnership is the Data Retention Directive adopted under the first pillar.

19. See Working Party 29 Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

20. Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal immigration, Prüm, 27 May 2005. The Prüm Treaty has been incorporated in the EU legal order.

21. Stockholm Programme, p. 36.



them. For this reason, and while the European Council 'notes with satisfaction that developments over the past years in the EU have led to a wide choice and created an extensive toolbox for collecting, processing and sharing information between national authorities and other European players in the area of freedom, security and justice',<sup>22</sup> where the principle of availability continues to give important impetus to this work, there is a need for a coherent and consolidated development of information management and exchange. In this respect, the European Council invites the Council and the Commission to adopt and implement an 'EU Information Management Strategy', and to consider the need for developing a 'European Information Exchange Model' based on current instruments, such as the Prüm framework and the so-called Swedish Framework Decision (Proposal for a Framework Decision on exchange of information under the principle of availability).

The Stockholm Programme stipulates that the EU information management strategy should be based among others on business-driven development (a development of information exchange and its tools that is driven by law enforcement needs), guiding principles for a policy on the exchange of information with third States for law enforcement purposes, interoperability of IT systems, a rationalisation of the different tools, including the adoption of a business plan for large IT systems, and overall coordination, convergence and coherence. The European Council also calls for the establishment of an administration having the competence and capacity to develop technically and manage large-scale IT-systems in the area of freedom, security and justice.

The European Council also takes into account and stresses the role of new technologies that need 'to keep pace with and promote the current trends towards mobility, while ensuring that people are safe, secure and free'.<sup>23</sup> In this respect, it invites the Council, the Commission, the European Parliament, and, where appropriate, the Member States to 'ensure that the priorities of the internal security strategy are tailored to the real needs of users and focus on improving interoperability'. Finally, it calls the EU institutions to reflect on how to develop further the use of existing databases for law enforcement purposes, while fully respecting data protection rules, so as to make full use of new technologies with a view to protecting the citizens.

---

22. Stockholm Programme, p. 38.

23. Stockholm Programme, p. 40.

**ii. Some caveats: why should we be careful when characterizing the EU as an emerging 'Surveillance society'?**

It has been argued that the EU is developing more and more elements of a surveillance society. However, the characterization of the EU as an emerging 'surveillance society' might be scientifically risky and thus requires several caveats. First of all, it is a known fact that the EU does not have police or public authorities with executive powers to ensure security directly. This means that its contribution to security is based on the adoption of measures that are intended to enable the competent authorities of the Member States to fight terrorism and crime themselves.<sup>24</sup> In this respect, the EU has laid down a number of legislative instruments aimed to harmonize, co-ordinate and facilitate the Member States' action against terrorism and crime.

Secondly, and within this context, the role of the EU as a "Surveillance society" comes *in principle* at a later stage: it is normally the national authorities of the Member States that will first collect the information using surveillance technologies, and the EU will then make the exchange of this information with other Member States as well as possible and its storage in centralized databases.

**IV. The EU as an emerging 'Surveillance society' and Data Protection: Dangers**

The protection of personal data is recognized in primary EU law as a dimension of the right to respect for private life<sup>25</sup> under Article 8 of the European Convention on Human Rights (ECHR), as reflected in Article 6 (2) of the TEU, which provides that the Union respects fundamental rights, as guaranteed by the ECHR and the constitutional traditions common to the Member States, as general principles of Community law'.<sup>26</sup>

---

24. Buttarelli, 'Legal Restrictions- Surveillance and fundamental rights' in 'New Technical Means of Surveillance and the Protection of Fundamental Rights- Challenges for the European Judiciaries', Vienna July 19th, 2009, p. 4.

25. Skandamis, Sigalas and Stratakis, 'Rival Freedoms in Terms of Security: The Case of Data Protection and the Criterion of Connexity', Research Paper No.7, December 2007, available at <http://www.ceps.eu>, p. 6.

26. The ECJ has repeatedly held with regard to fundamental rights that: 'fundamental rights form an integral part of the general principles of law whose observance the Court ensures. For that purpose, the Court draws inspiration from the constitutional traditions common to the Member States and from the guidelines supplied by international instruments for the protection of human rights on which the Member States have collaborated or to which

More importantly, the right to data protection, enjoys constitutional protection within the EU legal order enjoys as it is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (EUCFR). This elevation of the right to data protection to the level of a fundamental right is immensely or hugely very important, because, for the first time, it has been recognized as a distinct right from the right to respect for private and family life, home and communications, which is set out in Article 7 of the Charter.<sup>27</sup>

There is a particular danger posed to the fundamental right to data protection by the EU as an emerging 'surveillance society': the so-called 'function' or 'competence creep'. Within the EU legal context, this danger is linked to the EU's own particular nature that encompasses different competences in distinct areas. Most EU databases, such as VIS or EURODAC have nothing to do with the fight against terrorism or crime, since they have been created for different purposes. For instance, the Visa Information System was created to support the common visa policy, and EURODAC was established in order to enhance the common asylum policy. Yet, data contained in the former database can be accessed by designated authorities of Member States and by Europol to fight terrorism; the same - with even more serious consequences - has been proposed with respect to EURODAC. This raises many concerns: once the information has been collected and stored in centralized databases, it can be very easily used for law enforcement purposes. This is required in the name of the 'surveillance society'. However, the fundamental question here is: can new technologies information be used only because it exists: can and new technologies permit the storage of data and their interchange? In this respect, this article will take a closer look at the case studies of VIS and EURODAC.

## *i. 'Function creep': the case studies of VIS and EURODAC*

### **1. The case of VIS**

#### *a. The VIS legal framework*

Despite the fact that the Visa Information System database (VIS) has no direct connection with the EU's counter-terrorism strategy being a database that supports the common visa policy, ironically enough, as an author points out, the de-

---

they are signatories. In that regard, the ECHR has special significance'. See for instance Case 29/69 Stauder [1969] ECR 419, para 7.

27. Rodota, 'The European Constitutional Model for Data Protection', paper presented at the Public Seminar of the European Parliament: PNR/SWIFT/Safe Harbour: Are transatlantic data protected? (Transatlantic relations and data protection), Monday 26 March 2007, available at [http://www.europarl.europa.eu/hearings/20070326/libe/rodota\\_en.pdf](http://www.europarl.europa.eu/hearings/20070326/libe/rodota_en.pdf), p. 2.

cision to establish the Visa Information System (VIS) was 'a direct consequence of the terrorist attacks of 11 September'.<sup>28</sup> At the extraordinary Council meeting of 20 September 2001 that followed the attacks, the Home Affairs and Justice Ministers agreed that the procedures for the issue of visas should be tightened and that the Commission should make proposals for the establishment of a network for information exchanges concerning visas issued by Member States. The VIS would collect and store fingerprints and other biometric identifiers of all third-country nationals applying for short-term visas in any EU Member State. According to the relevant Council guidelines, the development of the VIS aimed, among others, to contribute towards improving internal security and combating terrorism.<sup>29</sup>

The Council Decision establishing a system of exchange of visa data between Member States, the 'Visa Information System', was adopted on 8 June 2004 on the basis of Article 66 EC.<sup>30</sup> The Decision gives the Commission the mandate to develop the VIS. It constitutes the required legal basis to allow for the inclusion of the necessary appropriations for the development of the system through EC financing. According to the Decision, the Visa Information System will be based on a centralised architecture and consists of a central information system, 'the Central Visa Information System' (CS-VIS), an interface in each Member State, 'the National Interface' (NI-VIS), which will provide the connection to the relevant central national authority of the respective Member State, and the communication infrastructure between the Central Visa Information System and the National Interfaces.<sup>31</sup> The Central VIS, the National Interface in each Member State, and the communication infrastructure between the Central VIS and the National Interfaces are to be developed by the Commission, while the national infrastructures are to be adapted and developed by the Member States.<sup>32</sup> The system will be designed to provide for the connection of at least 12,000 users in 27 Member States and at 3,500 consular posts.<sup>33</sup>

---

28. Baldaccini, 'Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases', (2008) *European Journal of Migration and Law* 10, 31, 39.

29. Council Conclusions on the development of the Visa Information System (VIS), Doc. 6535/04, 20 February 2004.

30. Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213/5.

31. Article 1 (2) of the VIS Decision.

32. Article 2 of the VIS Decision.

33. Communication from the Commission to the Council and the European Parliament – Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS), COM(2003) 771 final, 11 December 2003, p. 26.

Citizens from 134 countries require visas to enter the EU. This means that it had been possible for an applicant rejected by one country's consulate to continue applying to other consulates. Once the VIS is in place, this will no longer be possible. Information on previous applications and reasons for rejection will be available through the new system. The inclusion of fingerprint data is intended to allow the exact verification of somebody's identity.

The VIS was due to become operational by spring 2009. On 24 June 2009, following the request of the Council and the European Parliament, the Commission introduced a legislative package proposing the setting up of an Agency for the long-term operational management of the SIS II, VIS, EURODAC and other large-scale IT systems in the area of freedom, security and justice. According to the proposals, the core mission of the Agency would be to fulfil the operational management tasks for SIS II, VIS and EURODAC, keeping the systems functioning 24 hours a day, seven days a week. In addition to these operational activities, the Agency will also be responsible for adopting the necessary security measures, reporting, publishing statistics, the monitoring of research, SIS II and VIS related training and information issues. It will ensure data security and integrity as well as compliance with data protection rules.

In order to implement the Decision, a Regulation defining the purpose, the functionalities and the responsibilities of the information system, and establishing the procedures and conditions for the exchange of data between Member States on short-stay visa applications was adopted on 9 July 2008.<sup>34</sup> According to it, the data to be recorded in the VIS include not only alphanumeric data (on the application and on the visas requested, issued, refused, annulled, revoked or extended), but also biometric identifiers such as photographs and applicants' fingerprint data. Links to previous visa applications and to the application files of persons travelling together are also included in the VIS.<sup>35</sup>

Access to the VIS for entering, amending or deleting data, will be reserved exclusively to duly authorised staff of the visa authorities; access for consulting data will be reserved to visa authorities and authorities competent for checks at the external border crossing points, immigration checks and asylum, and will be limited to the extent the data is required for the performance of their tasks.

---

34. Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218/60.

35. Article 5 of the VIS Regulation.

*b. Counter-terrorism and access to VIS for law enforcement purposes: challenges to fundamental rights*

As seen above, apart from improving the implementation of the common visa policy, one of the purposes of VIS was also to contribute towards internal security and to combating terrorism. In its meeting of 7 March 2005, the Council stated that 'in order to achieve fully the aim of improving internal security and the fight against terrorism', Member State authorities responsible for internal security should be guaranteed access to the VIS, 'in the course of their duties in relation to the prevention, detection and investigation of criminal offences, including terrorist acts and threats'.

On 23 June 2008 the Council adopted a Decision allowing access for consultation of the Visa Information System by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.<sup>36</sup> The Decision was adopted on the basis that 'it is essential in the fight against terrorism and other serious crimes for the relevant services to have the fullest and most up-to-date information in their respective fields in order to perform their tasks. The Member States' competent national services need information if they are to perform their tasks'. In this respect, 'the information contained in the VIS *may be necessary* for the purposes of preventing and combating terrorism and serious crimes and should therefore be available for consultation' by the designated authorities,<sup>37</sup> and by Europol that has a key role in the field of cross-border crime investigation and in supporting Union-wide crime prevention, analyses and investigation.<sup>38</sup>

The Decision provides that VIS will be accessed by designated authorities of the Member States. For this purpose, every Member State must keep a list of the designated authorities and notify them to the Commission and the General Secretariat of the Council. The Commission will publish these declarations in the *Official Journal of the European Union*.<sup>39</sup> Access to the VIS for consultation can be ex-

---

36. Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218/129.

37. See Recital 3 of the VIS Decision (emphasis added).

38. See Recital 4 of the VIS Decision.

39. Article 3 of the VIS Decision.

exercised also by authorities responsible for internal security from Member States which are not part of the VIS.<sup>40</sup>

Access to VIS data is limited for the specific purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences, as referred to in Council Framework Decision 2002/584/JHA on the European arrest warrant. The Decision stipulates that 'it is essential to ensure that the duly empowered staff with a right to access the VIS is limited to those who 'have a need to know' and possess appropriate knowledge about data security and data protection rules'.<sup>41</sup>

Article 5 of the Decision lays down clearly the conditions for the access to VIS data. In order to exclude routine access, this provision allows for the processing of VIS data only on a case-by-case basis. Such a specific case exists in particular when the access for consultation is connected to a specific event or to a danger associated with serious crime, or to a specific person in respect of whom there are serious grounds for believing that he will commit or he/she or they has committed terrorist offences or other serious criminal offences or he has a relevant connection with such a person. In this regard, the designated Member States' authorities and Europol may search the data contained in the VIS when they have reasonable grounds to believe that such a search will provide information that will substantially assist them in preventing, detecting or investigating serious crime.<sup>42</sup>

It is true that the VIS Decision attempts to circumscribe with a number of data protection safeguards the access to VIS data by law enforcement authorities. However, it has been asserted that this measure is still very problematic from the point of view of the right to personal data protection. More precisely, there is a specific data protection principle that suffers particularly by the Decision granting access to VIS data: the purpose limitation principle.

The 'purpose limitation principle' – that is, according to the Data Protection Directive, the principle that establishes that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes<sup>43</sup> – is a fundamental principle of the EU data

---

40. Article 6 of the VIS Decision. The VIS Regulation does not apply to the United Kingdom and Ireland. Denmark has decided to implement it.

41. Recital 6 of the VIS Decision.

42. Article 5 of the VIS Decision. See also Recital 8.

43. Article 6 (1) (b) of the Data Protection Directive.

protection regime.<sup>44</sup> This is because an individual's informed consent to the collection and processing of his/her personal data is dependent on the information for about the purpose and use of those data.<sup>45</sup>

With regard to the storage of personal information to centralized databases, the importance of the purpose limitation principle for safeguarding the transparency and the legality of the use of the data and consequently of the individuals' fundamental rights cannot be stressed enough overemphasized. Within this context, the principle of purpose limitation prescribes that the scope and purpose of a database should strictly define the group of users who may lawfully access the database and process the data held on it. This principle commands that there be a strict nexus between the purpose of a data collection and the use that can be made of the data.

Given the importance of the purpose limitation principle, it becomes almost by definition that this principle should enjoy the highest level of protection within the context of the VIS information system. This fundamental principle, however, is rendered meaningless by the general trend to grant law enforcement authorities access to databases that have no law enforcement purposes whatsoever. With respect to VIS, it is unacceptable that it contains among its purposes stipulated in the Regulation itself a vague and open goal of contributing to the prevention of threats to Member States' internal security. The Visa Information System database cannot function by its nature as a 'multifunctional tool'. In this regard, it is very different from the SIS which pursues also law enforcement purposes, and includes alerts upon which certain executive action should be adopted. VIS on the other hand should be used only for the implementation of EU visa policy, and not for the fight against terrorism, or serious crime, or even illegal immigration. Once the purposes of a large-scale information system, where huge amounts of data are stored, are not clearly and restrictively defined, then the system is opened up for any possible purpose. It goes without saying that this 'function' or 'competence creep', where personal data collected for one specific purpose and

---

44. This applies to data protection law in general. As Gellman (Gellman, 'Privacy: Finding a Balanced Approach to Consumer Options', available at <http://www.cdt.org/privacy/ccp/consentchoice4.pdf>) notes a 'statement of purpose helps to strike a reasonable balance between the interests of record keepers and those of record subjects. It tells the record subject the consequences of disclosing data ... A purpose statement provides the data subject with information about the purpose for data collection, so that he or she can assess the benefits and risks of disclosure and make an informed decision. It also prevents a record keeper from using or disclosing information in ways that are not in accordance with the stated purpose ... The purpose specification principle has a self-balancing feature'.

45. Cannataci and Bonnici, 'The end of the purpose-specification principle in data protection?', (2010) *International Review of Law, Computers & Technology* Vol. 24, No. 1, 101, 101.



in order to fulfill one function, are used for completely different purposes, which are totally unrelated to the ones for which they were initially collected, constitutes a breach to the purpose limitation principle.

The need for law enforcement authorities to benefit from the best possible tools to identify the perpetrators of terrorist acts or other serious crime cannot be disregarded. Furthermore, it seems that the Decision granting access to VIS for law enforcement purposes sets out a number of data protection safeguards and in particular envisages only access on a case-by-case basis and not routinely. However, it has been asserted that the adoption of the VIS Decision itself violates the purpose limitation principle. Granting access to VIS in order to combat terrorism and serious crime constitutes a disproportionate intrusion in the privacy of travelers who agree on their data to be processed for the more purpose of obtaining a visa, and expect their data to be collected, consulted and transmitted, for that purpose only. What is more, since information systems are built for a specific purpose, with safeguards, security, conditions for access determined by this purpose, granting access for a purpose different from the original one would not only infringe the principle of purpose limitation, but could also render the above mentioned elements inadequate or insufficient.<sup>46</sup> It is very questionable to what extent measures that introduce exceptions to the purpose limitation principle, such as the VIS Decision, which allows law enforcement authorities and Europol access and use of the VIS data for other purposes than for which these data were collected and processed, can be adopted in the context of the fight against terrorism.

Finally, the fact that law enforcement authorities are granted access to such a vast amount of data entails the risk of profiling individuals on the basis of the information held on them into VIS. This might lead to an infringement of other fundamental rights beyond the right to privacy of the individuals concerned.<sup>47</sup>

## 2. The case of EURODAC

### *a. Legal framework*

EURODAC, which stands for *European Dactyloscopie*, is the European fingerprint database for identifying asylum seekers and irregular border-crossers established by Council Regulation 2725/2000 of 11 December 2000.<sup>48</sup> The objective of the

---

46. See in this respect Opinion of the EDPS on the VIS Decision, above n 216, 4.

47. For instance, violations of the principle of non-discrimination, of due process rights, of the freedom of movement.

48. Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316/1.

creation of the EURODAC system was to facilitate the application of the Dublin Regulation, which makes it possible to determine the Member State responsible for examining an asylum application, by comparing the fingerprints of asylum seekers and illegal immigrants. EURODAC enables Member States to identify asylum applicants and persons who have been apprehended while unlawfully crossing an external frontier of the Community. The system is based on the assumption that asylum seekers must apply for asylum in the first EU country in which they arrive and may be sent returned to another Member State if it can be proven that they have either passed through the border of another Member State or already lodged an application for asylum in that Member State. Thus, by comparing fingerprints, Member States can determine whether an asylum applicant or a foreign national found illegally present within a Member State has previously claimed asylum in another Member State, or whether an asylum applicant entered the Union territory unlawfully. EURODAC stores fingerprints of every applicant for asylum and of every alien who is apprehended in connection with the irregular crossing of an external border of a Member State, over the age of 14 years.

EURODAC is a database aimed to support the implementation of the common asylum policy by preventing 'asylum shopping'. In particular, the computerised system allows for the identification of third-country nationals who may have already lodged asylum applications in the EU and whose data were already enrolled by one Member State. Thus, when a Member State receives a hit reply, proving that an asylum seeker has applied for asylum before in another Member State, it will request the other Member State to take back the asylum applicant.

EURODAC consists of (a) the Central Unit equipped with a computerised fingerprint recognition system; (b) a computerised central database in which the EURODAC data is processed for the purpose of comparing the fingerprint data of applicants for asylum and of illegal immigrants; and (c) means of data transmission between the Member States and the central database.

*b. EURODAC and counter-terrorism: challenges to fundamental rights*

Following the general trend, started with VIS, the Member States have agreed that EURODAC should also be made accessible for law enforcement purposes in order to fight terrorism. A commitment to this effect had been made by the Interior Minister of the EU's six largest Member States at their G6 meeting in Heiligendamm, Germany, on 22-23 March 2006.<sup>49</sup> Furthermore, a paper discussed at

---

49. See House of Lords European Union Committee, 40th Report of Session 2005-06, *Behind Closed Doors: the meeting of the G6 Interior Ministers at Heiligendamm*, HL Paper 221, 19 July 2006.

the beginning of 2007 states the following concerning the use of EURODAC for enforcement purposes:

'Frequently, asylum-seekers and foreigners who are staying in the EU unlawfully are involved in the preparation of terrorist crimes, as was shown not least in the investigations of suspects in the Madrid bombings and those of terrorist organizations in Germany and other Member States (for instance, two of the five accused in German proceedings against the terrorist group "Al Tawhid", which prepared attacks against Jewish institutions in Berlin and Dusseldorf, were asylum-seekers)... Access to EURODAC can help provide the police and law enforcement authorities of the Member States with new investigative leads making an essential contribution to preventing or clearing up crimes.'<sup>50</sup>

Along the same line, the conclusions of the Mixed Committee of the JHA Council of 12-13 June 2007 considered that, in order to fully achieve the aim of improving security and to enhance the fight against terrorism, access under certain conditions to EURODAC should be granted to Member States' police and law enforcement authorities, as well as Europol. The Ministers therefore invited the Commission to present 'as soon as possible' an amendment to the EURODAC Regulation in order to allow for police access to the database.<sup>51</sup>

On 10 September 2009 the Commission adopted a proposal concerning access to EURODAC data by Member States law enforcement authorities and Europol for law enforcement purposes.<sup>52</sup> The proposal was justified by the Commission on the basis that fingerprint data is especially useful information for law enforcement purposes, as it constitutes an important element in establishing the exact identity of a person. 'The usefulness of fingerprint databases in fighting crime is a fact that has been repeatedly acknowledged'.<sup>53</sup> Fingerprint data of asylum seekers are collected and stored in the Member State in which the asylum application was filed, as well as in EURODAC. In fact, the Commission points out that in most Member States the law enforcement authorities have direct or indirect ac-

---

50. Common 18-months Presidency Programme on Police and Customs Co-operation, Council Doc. 5291/07 of 12 January 2007, 6.

51. Access to Eurodac by Member State police and law enforcement authorities – Council Conclusions. Available at: <http://register.consilium.europa.eu/pdf/en/07/st10/st10002.en07.pdf>.

52. Proposal of 10 September 2009 for a Council decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM(2009) 342 final.

53. Proposal for a Decision on EURODAC, above n 237, 2.

cess to their national databases that contain the fingerprints of asylum seekers for the purpose of fighting crime.<sup>54</sup>

According to the Commission though, while Member States successfully access asylum seekers fingerprints on a national level, access to asylum seekers fingerprint databases of other Member States is more problematic. This is because there is a structural information and verification gap since there exists no single system which enables law enforcement authorities to determine the Member State that has information on an asylum seeker. If a query of a national Automated Fingerprint Identification Systems (AFIS) using the Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly, in combating terrorism and crossborder crime (Prüm Decision), does not result in a 'hit', it is not certain that any information will be made available in a Member State. In this respect, according always to the Commission's proposal, law enforcement authorities may not only remain ignorant about whether or not information is available at all and in which Member State, but often also whether this information relates to the same person. This means, pursuant to the proposal, that without any action at EU level, the action of law enforcement authorities may become prohibitively expensive or may seriously jeopardise the application of the law because no further efficient and reasonable action to determine a person's identity can be taken. Moreover, the absence of the possibility for law enforcement authorities to access EURODAC to combat terrorism and other serious crime was reported as a shortcoming by the Commission in one of its Communications to the Council and the European Parliament.<sup>55</sup>

I will not comment on the Commission's justification concerning access to EURODAC by law enforcement authorities, which nevertheless is, at best, extremely weak. Turning to the substance of the proposal itself, this follows in most points the VIS Decision, examined above. In particular, it establishes a case-by case access to EURODAC and lays down a number of data protection safeguards, among which the proportionality and purpose limitation principles are included.

A number of points should be advanced on the EURODAC proposal. First of all, here again we are dealing with a function creep case. When adopted, the Regulation establishing EURODAC did not contemplate police access to EURODAC; the fingerprints were collected for the very specific purpose of determining which Member State is responsible for examining an asylum application, and in any

---

54. Proposal for a Decision on EURODAC, above n 237, 2.

55. Commission Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs of 24 November 2005.

case for facilitating the application of the Dublin Convention. To be used for a completely different purpose, that is by law enforcement authorities to fight terrorism and crime, it clearly goes against the purpose limitation principle and the legitimacy of the processing.

There are however wider concerns about access to EURODAC data for law enforcement purposes. The proposal for a Council Decision not only concerns individuals in principle not suspected of any crime, but what is more important, it concerns a particularly vulnerable group in society, i.e. asylum seekers, who are in need of higher protection because they flee from persecution.<sup>56</sup> Furthermore, granting access to EURODAC data to law enforcement authorities might have a discriminatory impact on asylum seekers, or other illegal border-crossers whose data are stored in the EURODAC database, in that they might be subject to 'a greater level of surveillance' than others in the population,<sup>57</sup> particularly as there is a general presumption that a disproportionate criminal activity might result from this group. This assumption is very dangerous to be translated into legal texts, since, besides reinforcing widespread prejudices, it also increases the risk of discrimination.

Finally, as the EDPS highlights in his Opinion, the Commission's proposal raises questions with regard to its necessity since there already exist a number of legal instruments,<sup>58</sup> concerning access to centralized databases by law enforcement authorities that have not yet been fully implemented.

---

56. See Opinion of the European Data Protection Supervisor on the Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], and on the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, para 17.

57. Baldaccini, above n 28, 44.

58. For instance, the Prüm Decision, provides that Member States shall grant each other an automated access *inter alia* to national Automated Fingerprint Identification Systems (AFIS). Also, Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ 2008, L 386/89) facilitates the exchange of information (fingerprints and supplementary information) which is held by or is available to law enforcement authorities in the Member States.

## **V. Concluding remarks: Law and Ethics in the modern 'EU Surveillance society': is it all about Security?**

It has been argued that one can identify, with a number of caveats, three elements of the surveillance society, i.e. 1) the increased engagement in intelligence gathering and surveillance activities, 2) the use of new technologies and technological devices, and 3) the overall goal of enhancing security in the EU's actions after 9/11 and especially after the Madrid and London terrorist attacks. Starting from this premise, the present contribution has focused on the examination of the so-called 'function creep' paradigm.

It is not only ethics, but also law that demand that personal information cannot be used for different purposes from the ones that it was initially collected only because it exists and new technologies permit its interchange. The selected case studies of the VIS and EURODAC database have demonstrated that access to them for law enforcement purposes clearly goes against the purpose limitation principle, which constitutes a fundamental principle of the EU data protection regime. This principle applies even if the information is further used for security purposes in order to fight terrorism.

Also, it seems that both in the cases of VIS and EURODAC, the boundaries between migration and asylum issues, border control, criminal law and counter-terrorism are becoming increasingly blurred in the emerging EU 'surveillance society'. This entails the risk that the movement of people across borders is conceived and treated more and more as a security issue and a potential criminal activity and that certain parts of the population, such as asylum-seekers or illegal border-crossers, or more generally third-country nationals are regarded as potential threats to security. In addition, fishing expeditions, profiling and discrimination practices can very easily arise with regard to the two databases examined.

In this respect, the present contribution maintains that access to EURODAC data should not be granted to law enforcement authorities, not even for the purpose of the fight against terrorism. There are already numerous possibilities for gathering information through SIS II and VIS (not to mention directly between Member States), that have not become fully operational yet. Hence, there is no reason to rush in this field. The 'death' of the data protection principles in the Area of Freedom, Security and Justice is currently not a fictional scenario. All the more, there are serious concerns about the respect of further fundamental rights (besides data protection) in the AFSJ. Unfortunately, it seems that this is becoming all the more an Area of Security.

# Inconsistencies in the regulation of anti-circumvention in the EU

---

---

Petroula Vantsiouri

---

---

## 1. Introduction

Of all the issues of copyright policy in the last twenty years, probably the most controversial has been the issue of technological protection measures (TPMs). TPMs constitute self-help mechanisms, such as copy protection for DVDs, password protection for online services, and encryption of television broadcast signals, which are designed to prevent acts of infringement and exploitation of intellectual property rights by controlling copying or access to works<sup>1</sup>. As it was anticipated that ways would be found to circumvent these copy and access controls, the legal systems of many countries provide TPMs legal support by giving to the right holders concerned specific protection when trying to enforce and manage their rights by technical means. These so-called anti-circumvention norms do not create or enlarge exclusive rights as such, but they enhance the exploitation and enforcement of exclusive rights by making it illegal either to circumvent TPMs or to offer services that enable circumvention<sup>2</sup>.

The establishment of legal regimes for the protection of TPMs was not an easy decision though. The adoption of anti-circumvention norms and the policies that they should serve have been very controversial issues. In the debate divergent opinions have been expressed regarding the form that anti-circumvention norms should take. The EU legislature resorted to three different formulas for EU anti-circumvention norms, according to the sector which TPMs protect. In particu-

- 
1. For a detailed definition and description of TPMs see K.J. Koelman & N. Helberger, 'Protection of Technological Measures' in P. B. Hugenholtz (ed.) *Copyright and Electronic Commerce* (1998), p. 168, 172; A. Strowel & S. Dusollier, 'La protection légale des systèmes techniques' in WIPO Workshop on Implementation Issues of the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT), WIPO doc WCT-WPPT/IMP/2, p. 2; J. De Werra, 'The Legal System of Technological Protection Measures under the WIPO Treaties, the Digital Millennium Copyright Act, the European Union Directives and other national laws (Japan, Australia)', Contribution to the ALAI 2001 Conference on Adjuncts and Alternatives to Copyright.
  2. M. Ficsor, *The Law of Copyright and the Internet, The 1996 WIPO Treaties, their Interpretation and Implementation*, (2002), p. 544; S. Ricketson & J. Ginsburg, *International Copyright and Neighbouring Rights, The Berne Convention and Beyond*, (2006), p. 965.

lar, anti-circumvention provisions can be found not in one or two, but in three Directives, namely in the Information Society Directive<sup>3</sup>, in the Software Directive<sup>4</sup> and in the Conditional Access Directive<sup>5</sup>. The Software Directive and the Information Society Directive protect copyright holders of computer programs and other works protected by copyright, including broadcasts, databases and performances respectively, whereas the Conditional Access Directive protects service providers from the unauthorized reception of their conditional access services, regardless of whether they contain works protected by copyright<sup>6</sup>.

During the legislative process of the three Directives the Commission did not identify any reasons that would justify the differentiation in the legal treatment of TPMs according to the sector to which they are applied, nor is there any technical evidence that TPMs work differently for different forms of subject matter<sup>7</sup>.

- 
3. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, O.J. L167, 22/06/2001 (henceforth Information Society Directive).
  4. Directive 2009/24/EC of the European Parliament and the Council of 23 April 2009 on the Legal Protection of Computer Programs, O.J. L111, 16, 05/05/2009 (henceforth Software Directive).
  5. Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, OJ L320, 28/11/1998 (henceforth Conditional Access Directive).
  6. A conditional access service is defined as television broadcasting, radio broadcasting or information society services, where provided on the basis of technical measures against remuneration and upon prior individual authorisation. See Article 2(a) and (b) Conditional Access Directive.
  7. On the legislative history of the three directives see: 1) Conditional Access Directive: Commission Green Paper 'on the Legal Protection of Encrypted Services in the Internal Market', Brussels, 06/03/1996, European Parliament: tabled legislative report, 1st reading, 15/04/1998, Official Journal C 152 18.05.1998, p. 0005. A4-0136/1998, COD/1997/0198: 30/04/1998 - EP: debates in plenary; 2) Software Directive: Green Paper on Copyright and the Challenge of Technology - Copyright Issues Requiring Immediate Action. COM (88) 172 final, 7 June 1988; Proposal for a Council Directive on the legal protection of computer programs, COM (88) 816 final, SYN 183, Submitted by the Commission on 5 January 1989, 89/C 91/05; Explanatory Memorandum; Amended Proposal of the Commission, COM (90) 509 final published OH No. C. 320. 20. 12. 90; Communication from the Commission to the Parliament SEC (91) 87 final. SYN 183 of 18.1.91; The Council's Reasons, Common Position Adopted by the Council on 13 December 1990 with a view to the adoption of a directive on the legal protection of Computer Programs, 10652/1/90. 3) Information Society Directive: *Europe and the Global Information Society- Recommendations of the High-level Group on Information Society to the Corfu European Council*, Brussels, 26 May 1994, p. 79; Commission Green Paper on Copyright and Related Rights in the Information Society, COM(95) 358 final, Brussels 19.07.1995; Commission Opinion pursuant to Article 251(2)(c) of the EC Treaty on the



Hence, one may assume that the existing differentiation among the anti-circumvention provision of the three Directives would be insignificant. On the contrary, the comparison among the anti-circumvention provisions found in the Information Society Directive, the Software Directive and the Conditional Access Directive indicates that there are important differences in the established legal regimes with regard to the prohibited acts, the *mens rea* of the infringer, the circumvention means, the protected technological measures, the relation of the anti-circumvention provisions to contract law and to the limitations of copyright law.

In that regard, this paper demonstrates the practical implications of the differences in the scope of application of the anti-circumvention norms according to the subject matter protected by TPMs. The paper concludes that there are great inconsistencies within the regulation of anti-circumvention, which demand a reevaluation of the policies that led to the adoption of the current form of EU anti-circumvention norms.

## 2. Differences in the regulation of anti-circumvention in the EU

### 2.1 *The prohibited acts*

With respect to the Software Directive and the Conditional Access Directive the legislature opted to address the problem of circumvention at its source and solely target the intermediaries that enable consumers to circumvent TPMs instead of going against the wider public, in light of the enforcement and marketing issues that would be raised, whereas that protection was not deemed to be adequate for the protection of copyright works. Thus, the Information Society Directive condemns both circumvention *per se* and trafficking in circumvention devices, whereas the Software Directive and the Conditional Access Directive do not pro-

---

European Parliament's amendments to the Council's common position regarding the proposal for a Directive of the European Parliament and of the Council on the harmonization of certain aspects of copyright and related rights in the information society, COM (2001) 170 final, Brussels 29.03.2001; Proposal for a European Parliament and Council Directive on the harmonization of certain aspects of copyright and related rights in the Information Society, Explanatory Memorandum, (henceforth Explanatory Memorandum) COM(97) 628 final, Brussels, 10.12.1997 and its Explanatory Memorandum; Common Position (EC) No 48/2000 of 28 September 2000 adopted by the Council, acting in accordance with the procedure referred to in Article 251 TEC with a view to adopting a European Parliament and Council Directive of the European Parliament and of the Council on the harmonization of certain aspects of copyright and related rights in the information society, OJ C 344, 01/12/2000; Legislative resolution embodying Parliament's opinion on the proposal for a European Parliament and Council Directive on the harmonization of certain aspects of copyright and related rights in the Information Society, OJ C 150, 28/05/1999, p. 0170 Amended Proposal, OJ C 180, 25.6.1999.

hibit the act of circumvention as such<sup>8</sup>. In other words, the EU anti-circumvention norms condemn viewers that circumvent copy controls embedded in DVDs featuring movies but they do not target either computer program users that circumvent TPMs to copy software, or viewers that circumvent TPMs embedded in their pay-TV decoders.

Equally significant are the differences in the scope of application of the anti-circumvention norms of the three Directives with regard to the wrongful acts that facilitate circumvention. The Information Society Directive requires Member States to censure the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of circumventing devices of both access and rights controls<sup>9</sup>. The Conditional Access Directive targets solely commercial acts that facilitate the circumvention of access controls<sup>10</sup> and the Software Directive condemns “any act of putting into circulation or the possession for commercial purposes” of circumventing devices<sup>11</sup>.

Hence, the “possession of circumventing devices of access controls for commercial purposes” is the only wrongful act targeted by all three Directives. Illustrating how limited the common scope of application of the three Directives is, an example of such unlawful acts presents the possession of devices that circumvent access controls protecting computer programs or copyright works or the possession of illicit pay-TV decoders by a provider of a website that offers unauthorised copies of songs, films, computer programs and TV broadcasts. Still, there is ambiguity regarding the meaning of the term “commercial use”, which may create confusion and differentiation among the interpretation of the term in the context of the three Directives. In particular, the notion of “commercial use”, which is not defined in the Software or the Conditional Access Directive, could vary from profit making purposes to any economic advantage<sup>12</sup>.

---

8. Compare Article 6(1) Information Society Directive to Article 7(1)(c) Software Directive and Article 4 Conditional Access Directive. Also see Report from the Commission on the implementation and effects of Directive 91/250/EEC on the legal protection of computer programs, COM (2000) 199 final, p.181, Commission Staff Working Paper, p. 9.

9. “Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes...” Article 6(2) Information Society Directive.

10. Article 4 of the Conditional Access Directive targets the “manufacture, import, distribution, sale, rental or possession”, the “installation, maintenance or replacement” and the “use of commercial communications to promote illicit devices” for commercial purposes.

11. Article 7(1)(c) of the Software Directive.

12. The term “commercial use” appears in the Rental and Lending Rights Directive, the Information Society Directive and the Enforcement Directive. Article 1(3) Rental and Lending Right

However, the differences in the types of acts targeted by the three directives are far more significant. On the one hand, the Software and the Information Society Directives have a broader scope of application in comparison to the Conditional Access Directive, to the extent that the act of “putting into circulation”, and the “manufacture, import, distribution, sale, rental, advertisement for sale or rental” do not need to be conducted for commercial purposes<sup>13</sup>. A computer expert who loans to her friends a circumventing device for TPMs embedded in music CDs or CDs with computer programs is infringing the norms of the Information Society Directive and the Software Directive, regardless of whether she receives any direct or indirect economic advantage; in contrast thereto, the computer expert is not liable according to the norms of the Conditional Access Directive, if she loans to her neighbors her illicit pay-TV decoder.

On the other hand, the Software Directive has a more limited scope of application in comparison to the other two Directives to the extent that it does not target acts such as the “advertisement for sale or rental” or the “use of commercial communications” to promote circumventing devices or services<sup>14</sup>. Hence a website that advertises devices circumventing TPMs that protect computer programs is not infringing according to the anti-circumvention norms of the Software Directive. Furthermore, in contrast to the Information Society Directive, the Software Directive does not target the manufacture and import of circumventing devices for non commercial purposes, when such devices are not subsequently put into circulation<sup>15</sup>. In other words, the owner of copyright in computer programs cannot make use of the anti-circumvention provisions, when an end user of a program manufactured or imported a circumventing device, unless the copyright owner can prove, for example, that the end user loaned the device to third parties.

---

Directive defines non-commercial purposes in circumscribing the public rental right as the making available for use, for a limited period of time and “for direct or indirect economic or commercial advantage”. It has been suggested construing the requirement of commercial use according to the Enforcement Directive. See M. Walter, ‘Enforcement Directive’ in Walter & Von Lewinsky (eds.) *European Copyright Law, A Commentary*, (2010), p. 1459.

13. Article 4(a),(b) and(c) of the Conditional Access Directive. However, many Member States, such as Belgium, France, Italy, Poland and Spain chose to additionally sanction private use of illicit devices. See Recital 21 Conditional Access Directive and KEA & Cerna, Study of the impact on the Conditional Access Directive, study prepared on behalf of the European Commission, December 2007, available at: <[http://ec.europa.eu/internal\\_market/media/docs/elecpay/study\\_en.pdf](http://ec.europa.eu/internal_market/media/docs/elecpay/study_en.pdf)>.
14. Compare Article 7(1)(c) of the Software Directive with Article 6(2) of the Information Society Directive and Article 4(c) of the Conditional Access Directive.
15. Compare Article 7(1)(c) of the Software Directive with Article 6(2) of the Information Society Directive and Article 4(a) of the Conditional Access Directive.

Summing up, only the Information Society Directive condemns the act of circumvention *per se*, whereas all three Directives target the making and dealing in devices that facilitate circumvention. Still, the scope of the European anti-circumvention provisions as regards the prohibited acts differs to a considerable degree. The anti-circumvention provisions of the Information Society Directive have the broader scope of application of the three, whereas the Software Directive has a broader scope of application in comparison to the Conditional Access Directive as regards the circulation of circumventing devices, but a narrower scope of application as regards the manufacture, import and advertisement of circumventing devices.

## 2.2 *The mens rea of facilitators of circumvention*

Another difference of great significance among the anti-circumvention provisions of the three Directives concerns the required *mens rea* of the infringer. A distinction should be made between the required intent of circumventors of TPMs and the intent of people facilitating circumvention, as the two prohibitions target different groups of people and thus the interests that need to be protected by the legal order in each case differ. In particular, the actual circumventors of TPMs are the users of copyright works, the majority of whom may not have the technological knowledge to circumvent a TPM. In contrast thereto, the facilitators of circumvention are usually professionals or computer experts who manufacture or distribute circumventing devices and assist users to circumvent TPMs. As circumventing devices and services may also have additional non-infringing uses, it is crucial to determine under which circumstances the manufacturer or distributor of such devices is deemed to be infringing the anti-circumvention norms of the three directives.

The three Directives have taken completely different approaches with regard to the required intent of the persons facilitating circumvention of TPMs<sup>16</sup>. According to the Information Society Directive, if the means that facilitate circumvention have no other or only a limited commercially significant use other than to circumvent, then the *mens rea* of the person facilitating circumvention is irrelevant<sup>17</sup>. Thus, if a device is primarily used for unauthorised circumvention of TPMs, but can be used for other legitimate purposes, a person commits an of-

---

16. As regards the required intent for the act of circumventing *per se*, which is targeted only by the Information Society Directive, only the intentional act of circumvention is condemned, as the infringer circumvents the TPM “in the knowledge, or with reasonable reasons to know, that he or she is pursuing that objective”. See Article 6(2)(b) Information Society Directive.

17. “Member States shall provide adequate legal protection against the manufacture [...] of devices [...] which [...] or have only a limited commercially significant purpose or use other

fence by manufacturing and selling such a device, even if the device was genuinely manufactured or sold for legitimate purposes. If the means facilitating circumvention have a commercially significant use other than to circumvent, the anti-circumvention provisions implementing the Information Society Directive are infringed when someone promotes, advertises or markets those means with the intent that they are used for the purpose of circumvention, or she designs, produces, adapts or performs them with the intent that they are used primarily for the purpose of enabling or facilitating circumvention of any effective TPMs<sup>18</sup>.

As regards the Software Directive, it has been argued that the distribution or possession of TPMs as an instance of vicarious liability does not presuppose intention or negligence, as long as the articles concerned are specifically intended to facilitate the removal or circumvention of any technical means that have been applied to protect a computer program<sup>19</sup>. However, this statement appears to contradict itself. The required *mens rea* of the infringer is predicated on whether the “sole intended purpose” should be found according to the understanding of a third party, for example, a neutral observer or the average distributor of anti-circumvention devices or according to the intent of the actual distributor of anti-circumvention devices. The wording of the provision which refers to “sole intended” and not to “sole commercially significant” purpose, for example, supports the second interpretation. Thus, liability according to the Software Directive is always predicated on *scienter* (*dolus malus*), and in particular, the distributor of the device must intend it to be used by a third party to circumvent a TPM.

Finally, the Conditional Access Directive does not require Member States to outlaw only the intentional facilitation of illicit devices, but it provides Member States with the discretion to condemn the commercial manufacture, distribution and promotion of infringing equipment or software, only if those activities are

---

than to circumvent [...] any effective technological measures. Article 6(2)(b) of the Information Society Directive. (emphasis added).

18. “Member States shall provide adequate legal protection against the manufacture [...] of devices [...] which (a) are promoted, advertised or marketed for the purpose of circumvention of, or[...] or (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.” Article 6(2)(a) and (c) and Recital 48 of the Information Society Directive. (emphasis added).
19. *Kabushiki Kaisha Sony Computer Entertainment Inc v Ball* [2004] EWHC 1738 (Ch); (2004) ECDR 33, 323; (2005) FSR 9; (2005) ECC 24; W. Blocher & M. Walter, ‘Computer Program Directive’ in Walter & Von Lewinski (eds.) *European Copyright Law, A Commentary*, (2010) p. 196, 205.

carried out in the knowledge or with reasonable grounds to know that the devices in question were illicit<sup>20</sup>.

The legislative choice to outlaw the unintentional facilitation of circumvention has significant practical consequences on technological innovation. An electronics retailer who offers for sale components necessary to assemble a device that circumvents TPMs embedded in music CDs is liable for facilitation of circumvention, if those components are primarily used by the public to circumvent TPMs, regardless of whether the retailer is unaware of the destination of the components or whether she promoted them for other lawful uses. In contrast thereto, if the electronic components are used to assemble a device that circumvents TPMs which protect computer programs and those components have any other lawful use other than to circumvent effective TPMs, the retailer is liable only if she is distributing the components with the intention to facilitate the circumvention of TPMs. Thus, the choice to outlaw the unintentional facilitation of circumvention under the Information Society Directive and also potentially under the Conditional Access Directive, causes uncertainty within the markets for electronics and inhibits the development and circulation of technologies with additional beneficial uses. In contrast thereto, owners of copyright in computer programs bear the additional burden to prove that distributors and possessors of circumventing devices intended that the devices were used to circumvent TPMs, which, however, may fuel innovation.

## **2.3 The means of circumvention**

### **2.3.1 The purpose served by circumventing means**

The analysis above of the required *mens rea* for the infringement of the anti-circumvention provisions targeting preparatory acts has already highlighted a significant difference between the Information Society, the Software and the Conditional Access Directives as regards the types of circumvention devices or services that fall under their scope. According to Article 6(2)(c) of the Information Society Directive a device or service is considered infringing the anti-circumvention norms if its “primary purpose” is to enable or facilitate circumvention of TPMs, whereas pursuant to Article 7(1)(c) of the Software Directive if its “sole intended purpose” should be to facilitate circumvention. A device or service that has an intended purpose other than the unauthorised removal or circumvention of TPMs

---

20. See Recital 22 Conditional Access Directive. See also Decision No. 2002/13661 of the Paris Court of Appeals of 21 May 2003, which convicted a couple sued by the French pay-TV operator Canal+ for offering for sale the components necessary to assemble a pirate decoder, despite the couple's assertion that they completely ignored the destination of the components that they were promoting and selling.

applied to computer programs, for example to allow software programmed to operate with Windows also to operate with Linux, does not violate the anti-circumvention norms. However, the same device may be considered infringing, if it circumvents TPMs applied to works other than computer programs, as in that case the copyright holder needs to prove the lower “primary purpose” standard, namely that the device is primarily designed to enable or facilitate circumvention, regardless of whether it may also have intended secondary legal uses<sup>21</sup>. Finally, an “illicit device” does not need to satisfy even the lower “primary purpose” standard in order to invoke the application of the Conditional Access Directive, since “any equipment or software designed or adapted to give access to a protected service” falls within the scope of the provision<sup>22</sup>. Thus, potential legal uses of an “illicit device” are of no importance for the application of anti-circumvention provisions protecting conditional access services<sup>23</sup>.

### 2.3.2. The nature of circumventing means: devices or services

Another important difference regarding the scope of application of the EU Directives regards the nature of circumventing means as encompassing services. This distinction is of great significance as the Software Directive and the Conditional Access Directive do not target the act of circumvention *per se*. Still, a professional who circumvents TPMs that protect computer programs or conditional access services for the benefit of third parties could be held liable if the offer of circumvention services for commercial purposes was condemned. This is not the case though for the Conditional Access Directive, whereas there is disagreement as

21. See also *Sony Computer Equipment v Owen* (2002) E.C.D.R. 286.

22. Article 2(e) Conditional Access Directive.

23. See OLG Frankfurt, judgment of 05.06.2003, 6U 7/03 – Magic Modul, which held that a device sold for lawful purposes, and which did not advertise for its potential unlawful aptitudes could be considered an illicit device. The Hamburg Court of Appeals went even further with its subsequent decision OLG Hamburg, judgment of 08.02.2006 and held that developers of software that enable users to infringe pay-TV services should do everything necessary and reasonable to avoid infringement by users, such as implementing an appropriate DRM. In contrast thereto, in Sweden and Denmark illicit devices need to be sold for the purpose of illegally decoding Conditional Access Services. However, recent case-law in Sweden reversed the burden of proof and held that when there is a massive sale of blank cards, even when they can be used for legitimate purposes, it can be presumed that their purpose of sale is for illegally decoding conditional access services. (*State v. Keycard*, Case 2004:17, Dnr C 4/03, June 30 2004). See Kea & Cerna, Study on the Impact of the Conditional Access Directive, Study prepared on behalf of the European Commission, p. 93-97 (December 2007), available at: <[http://ec.europa.eu/internal\\_market/media/elecpay/index\\_en.htm#study](http://ec.europa.eu/internal_market/media/elecpay/index_en.htm#study)>.

to whether the scope of application of the anti-circumvention provisions of the Software Directive extends to services.

The Information Society Directive explicitly targets “devices, products or components or the provision of services”<sup>24</sup>. An equally elaborate definition of “illicit devices” is included in the Conditional Access Directive, which instructs Member States to prohibit commercial acts regarding “any equipment or software designed or adapted to give access to a protected service”<sup>25</sup>. Thus the scope of application of the Information Society Directive is broader to the extent that it also targets services enabling circumvention, whereas the Conditional Access Directive targets solely devices and code. In contrast thereto, the Software Directive targets “any means facilitating the unauthorised removal or circumvention of TPMs” without providing any further explanation regarding the meaning of the term. The broad term “any means” logically encompasses “devices, products, or components” within the meaning of Article 6 of the Information Society Directive<sup>26</sup>. However, there is disagreement as to whether the expression “any means” as used in the text of the Software Directive, extends to services.

Hence, although all three Directives target the provision of devices facilitating circumvention, only the Information Society Directive elaborately condemns the provision of circumvention services. The Conditional Access Directive does not target facilitators of circumvention who offer their services to third parties, whereas there is legal uncertainty as to whether services are fall within the scope of application of the Software Directive.

#### ***2.4. Exceptions and Limitations to Copyright***

The most common criticism against TPMs is that they frequently block non-infringing uses of copyright works. A number of scholars have examined the consequences of anti-circumvention regulation on the privileges enjoyed by end users according to “traditional” copyright law and they struggled with the question of whether and how anti-circumvention law could better accommodate copyright

---

24. Article 6(2) Information Society Directive.

25. Article 2(e) Conditional Access Directive.

26. L. Bently, ‘Directive 91/250/EEC – Directive on the legal protection of computer programs’ in Dreier & Hugenholtz, *Concise European Copyright Law* (2006); Blocher & Walter, *supra* note 19, p.204. Cf Supreme Court of Finland of 3 October 2003 *Adobe Systems v A Software Distributor* [2004] ECDR 30, 303, which held that instructions in writing enabling installation of program updates did not fall within the scope of the corresponding provision of the Finnish Copyright Act.



exceptions<sup>27</sup>. On such an important issue, the EU legislature has taken different stands as to the extent and the method that exceptions and limitations of copyright are accommodated under each Directive.

The Information Society Directive requires the protection of all TPMs that prevent or restrict uses or access not authorised by the right holders, regardless of whether the users attempting access or use can take advantage of some of the exceptions established in Article 5 of the Directive. Article 6(3) of the Information Society Directive defines TPMs as technologies designed to prevent or restrict acts “which are not authorized” by the concerned rightholders and thus it makes no reference to the technological measures that impede violation of copyright.

As a response to concerns regarding the expansion of the right of copyright holders to the detriment of the public, the Information Society Directive encourages right holders to provide a voluntary mechanism in order to make available to beneficiaries of certain exceptions permitted under the Directive the means of benefiting from them and it requires member states to ensure that right holders do in fact make available such means<sup>28</sup>.

However, the Information Society Directive provides an exclusion from this requirement for “works or other subject matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them”<sup>29</sup>. This provision effectively annuls the established voluntary method of addressing copyright ex-

---

27. Indicatively see P. Akester, ‘Technological Accommodation of Conflicts between Freedom of expression and DRM: the first empirical assessment’, (CIPIL 2009) available at <<http://www.law.cam.ac.uk/faculty-resources/download/technological-accommodation-of-conflicts-between-freedom-of-expression-and-drm-the-first-empirical-assessment/6286/pdf>>, N. Braun, ‘The Interface between the protection of the Technological Measures and the Exercise of Exceptions to Copyright and Related Rights: Comparing the Situation in the United States and the European Community’, 25 *European Intellectual Property Review* 496 (2003); D. Burk & J. Cohen, ‘Fair Use Infrastructure for Rights Management Systems’, 15 *Harvard Journal of Law & Technology* 41 (2001); S. Dusollier, ‘Tipping the Scale in Favour of the Right Holders: The European Anti-Circumvention Provisions’, in E. Becker, W. Buhse, D. Günnewig, N. Rump (eds.) *Digital Rights Management. Technological, Economic, Legal and Political Aspects* (2003), p.462; K. J. Koelman, ‘A Hard Nut to Crack: the Protection of Technological Measures’ 22(6) *EIPR* 272 (2000); J. Litman, *Digital Copyright* (2006), Chapter 9; T. C. Vinje, ‘A Brave New World of Technical Protection Systems: Will There Still be room for copyright’, 18 *EIPR* 431 (1996).

28. Article 6(4)(1) Information Society Directive. In addition, Article 12(1) instructs the Commission to examine and report on a triennial basis “whether the acts which are permitted by law are being adversely affected by the use of effective technological measures”.

29. Article 6(4)(4) Information Society Directive.

ceptions in the online environment, as the norm is that online applications allow members of the public to access works from a place and time individually chosen by them, after they have agreed to standard form contractual provisions (take-it-or-leave) set out by the provider of the work<sup>30</sup>. In short, the Information Society Directive privileges a rule of prevalence of contract over exceptions in the online environment.

For example, an academic who wants to copy parts of a movie for her class cannot raise the defence of “illustration for teaching” against the owner of the copyright in the movie and circumvent the TPMs that protect it. In such a case, the copyright holder is encouraged to take voluntary measures to accommodate the needs of the teacher, or else the Member State where this incident occurs shall take appropriate measures to ensure that right holders make available to the teacher the means of benefiting from that exception. However, if the protected movie is streamed online through a conditional access service, the copyright holder bears no obligation to take voluntary measures to accommodate the needs of the teacher.

As regards the Software Directive, it has been argued that Article 7(1)(c) applies also in cases where the means of circumvention are used only in order to carry out acts that do not require authorisation on the ground of an exception of a restrictive act<sup>31</sup>. The reasoning, which was also adopted by the High Court of England & Wales in *Sony v Ball*, is that in cases where circumvention takes place to enable the exercise of an exemption, the “sole intended purpose” of the device remains circumvention and circumvention is “unauthorised”. Thus, Article 7(1)(c) is not limited to situations where the person knows or has reasons to believe that the means will be used to make infringing copies<sup>32</sup>. However, this reasoning does not explain what the word “unauthorized” adds to the meaning of the provision. If the legislator wished to exclude from the scope of Article 7(1)(c) only circumvention devices which have more functions, other than to circumvent, such as a personal computer, the provision would target devices the sole intended purpose of which would be to facilitate circumvention. The inclusion of the term “unauthorised” establishes a requirement that the copyright holder must have the power to prohibit circumvention on a basis other than the anti-circumvention provisions, such as copyright or contract law. The wording of the provision suggests that there should be a link between copyright infringement and infringement of the anti-circumvention provisions and, thus, exceptions to copyright should be

---

30. See also Recital 53 Information Society Directive.

31. Bently, *supra* note 26, p. 235; Blocher & Walter, *supra* note 19, p. 205.

32. *Ibid*; See also *Kabushiki Kaisha Sony Computer Entertainment Inc v Ball*, *supra* note 19.

regarded as prevailing over the anti-circumvention norms established by the Software Directive. It is likely that the interpretation followed by the High Court was prompted by policy considerations. If the provision had been limited to situations where the person knows or has reasons to believe that the means will be used to make infringing copies, there would have been pragmatic difficulties in applying it to computer programs.

Furthermore, the Software Directive establishes a rule that certain exceptions will prevail over contractual terms, so that contractual provisions contrary to the exceptions referred to in Articles 5(2) and (3) and 6 are deemed null and void<sup>33</sup>. Thus, the making of a back-up copy, the observation, study or testing of the functioning of a computer program and decompilation to achieve interoperability are raised to the level of guaranteed rights of access and use, which cannot be bypassed by contractual provisions offering more protection to copyright holders.

Finally, the Conditional Access Directive does not contain within its text any limitations, or any provision regarding its relationship to copyright exceptions. The lack of explicit mention of copyright limitations led commentators to interpret Recital 21 of the Directive, which states that the Directive is without prejudice to the application of intellectual property rights, as signifying that the Directive is also without prejudice to any exceptions to intellectual property rights. Hence the relationship between the Conditional Access Directive and copyright exceptions would be unclear<sup>34</sup>. However such an interpretation disregards the scope of application of the Conditional Access Directive and the nature and scope of application of copyright exceptions. The copyright exceptions and limitations are defences that a defendant may rely upon when sued for copyright infringement. Hence they may be raised *vis-a-vis* copyright holders, and not towards third parties. They do not constitute an absolute right for users of copyright works. On the contrary, they allow certain uses of copyright works, which would otherwise infringe the copyright of protected works. Thus, users could raise the defence against broadcasters that they benefit from copyright exceptions, only to the extent that broadcasters raise claims based on infringement of their copyright on the broadcasts or as licensees of the copyright holders. However, the object of protection of the Conditional Access Directive is the remunerated service and not copyright. Since broadcasters enjoy a distinct right to remuneration based on a different legal basis than copyright law, the exception to copyright cannot extend its application beyond the scope of copyright law. Furthermore, as the services in question are protected also when their content is not protected by copyright at

---

33. Article 8(2) with Articles 5(2), 5(3) and 6 Software Directive.

34. T. Heide, "Access Control and Innovation under the Emerging EU Electronic Commerce Framework", 15 *Berk.Tech.L.J.* 993 (2000), 1018, 1043.

all, logic dictates that those services will be protected also when their content is a copyright work, but users can benefit from an exception.

#### 4. Conclusion

While the need for protection of TPMs is unequivocal according to European anti-circumvention norms, in practice, the degree of protection for TPMs varies according to the protected subject matter and is often uncertain, as the wording of the anti-circumvention provisions in the EU is complex, difficult to interpret and in some cases contradictory. Only the Information Society Directive targets the act of circumvention *per se* and the targeted preparatory acts to circumvention also differ under the three Directives. The rules clarifying the required *mens rea* of the facilitator of anti-circumvention as well as the characteristics of the circumventing means differ under the norms of the three Directives. Finally, the European legislature took different approaches to the question of whether exceptions to copyright should prevail over the anti-circumvention norms and any contractual arrangements or vice versa.

The differences in the scope of application of anti-circumvention norms according to the protected subject matter reflect different underlying policies that dictated the adoption of the one or the other approach. The choice to pursue the goals of anti-circumvention by targeting organized intermediaries who facilitate circumvention or the public who use the means made available to them entails the question of whether we should promote a “sheriff prosecution system”; on the one hand, it is more effective in shaping the conscience of the public that circumventing TPMs is illegal and thus will lessen the demand for devices and services that enable circumvention. On the other hand, it raises enforcement and proportionality issues as only an insignificant part of the infringers can be prosecuted, and thus those people will be treated as scapegoats to “scare” the rest of the public and make it conform to the “demands” of the law. Secondly, the approach taken under the Software Directive not to target the use of commercial communications aims to ensure the freedom of speech that media should enjoy and tries to relieve them from the burden of checking if what they publicise infringes anti-circumvention norms or not. A third issue of major importance is whether the anti-circumvention norms should make their enforcement easier for right holders at the cost of impeding technological innovation or vice versa. In particular, the lack of a required *mens rea* for the facilitators of circumvention and the adoption of “primary purpose” instead of “sole intended purpose”, as the criterion that a device should serve in order to fall under the definition of circumventing device according to the Information Society Directive, reflect a policy choice to broaden the scope of application of the anti-circumvention provisions to entail devices and services with beneficial uses that can contribute to technological innovation;

In contrast thereto, the legislature opted to allow the production and use of such devices under the Software Directive, at the cost of making the enforcement of its anti-circumvention norms less effective. Potential infringers may claim that their devices have other uses and right holders bear the additional burden to prove that the infringers were aware of the circumventing function of their devices or services. Finally, the prevalence of anti-circumvention provisions over user exceptions and limitations and contract law or vice versa is a hotly debated issue that is dealt with differently under each Directive and which allegedly affects the balance that copyright law should serve. Those concerns can be answered only after a re-evaluation of the policies that led to the adoption and to the current form of anti-circumvention norms. There is a need to explore whether different policy reasons dictate the different scope of anti-circumvention norms according to the protected subject matter, or whether the indicated differences are a result of inconsistent and inefficient protection of TPMs.

# **“All that is solid melts into air”: the history of copyright as a form of industrial regulation and its disorientation in the age of information**

---

---

**Nikolaos Volanis**

---

---

## **1. Introduction – Of “wars” and “pirates”**

“Intellectual Property is the oil of the 21st century” - this quote by Mark Getty, chairman of Getty Images, one of the world’s largest owners of intellectual property, presents an acute view on the current tension regarding intellectual property, particularly copyrights and patents. Not only does it present the crucial importance of informational assets in a knowledge-based economy, but it also alludes to the wars that have already been and will continue to be fought over ownership and appropriation of intellectual resources which are essential in a society. Some of those are named the “copyright wars”, which pertain to the “war” on “piracy,” which “threatens” the “survival” of certain important content industries (Lessig L., 2008, p. xvi): After all, one cannot forget the aphorism by the former head of the Motion Picture Association of America, Jack Valenti, that he is fighting what he called a “terrorist war” against “piracy” (Harmon A., 2002).

The selection of the word “war” seems not to have been made at random by the content industries. As Professors George Lakoff and Mark Johnson describe, every appearance of this word produces a “network of entailments”, which frame and drive social policy. Going to war means “*setting targets*”, “*reorganizing priorities*”, “*gathering intelligence*”, “*marshaling forces*”, “*imposing sanctions*”, “*calling for sacrifices*”, e.tc.. “*The WAR metaphor (...) was not merely a way of viewing reality; it constituted a license for policy change and political and economic action. The very acceptance of the metaphor provided grounds for certain interferences: there was an external, foreign, hostile enemy (...); energy needed to be given top priorities; the populace would have to make sacrifice*” (Lakoff G., and Johnson M., 1980, p. 156-57)

In this context, “wars” have been “waged” on the copyright battlefield, on the issue of how should law and policy regulate the interests of the creators of information vis-à-vis the interests of society. In general, the key assumption that sustains copyright law is that authors have a natural right over their works of intellectual labor, and copyright protection is required to provide an incentive to create intellectual works. It is argued that in the absence of a system like copy-

right, there would be no incentive for authors to produce and, hence, creativity and art will gradually diminish and decline. Moreover, copyright is based on a balance between the protection of authors, on the one hand, and the interests of the public, on the other (the so-called “copyright bargain”). For example, since excessive protection may result in curbing the public ability to use works, copyright protects only unique expressions and not ideas per se, and it is also provides a limited term of protection. Within these limits, any person who uses the works of another person’s intellectual labor without permission is infringing that person’s exclusive rights.

Facing the heated debate over the role of copyright in the era of digital network environments, people today tend to think of the above “war” as a new event and as a consequence of the rapid digitalization of knowledge. However, “wars” for ownership over information appear throughout the course of history in a recurring cycle; a cycle which reveals itself at specific intervals of societal evolution, when the introduction of a disruptive technology challenges the established privileges of certain groups, who at the time have acquired control of the means of information production. This pattern first became apparent with the introduction and spread of the printing press in the 1500s, but it re-emerges whenever a new and disruptive technology offering unprecedented capabilities for creation and production of cultural materials is introduced: the introduction of player pianos, gramophone, radio, television, VCRs, MP3 players, and, of course, the Internet, are only examples of such technology, each one prompting an after thought copyright policy, legislation or case law, in order to figure how the changes in technology will be transfigured into acceptable social or legal norms.

Amidst this debate over the role of copyright legislation in the age of networked information economy, we attempt an examination of the interrelationship between copyright policy and legislation and the methods of cultural production in the past, in order to compare it with the trends and objectives of copyright law-making and policy in the present taking into account the impact of technological innovation of our time. For this aim, our paper is divided in the following parts: a. the examination whether the above assertion that copyright protects the rights of authors is consistent with the very origins of copyright legislation in Europe and the US; b. the consideration how copyright regulation in the 20<sup>th</sup> century was amended to fit the established industrial processes of intellectual production and c. the estimation whether the above “balance” between the owners of information and society is still maintained, in light of changes to the model of intellectual production in the 21<sup>st</sup> century.

## 2. Copyright and the printing press

### *2.1 Censorship and control of knowledge in 16th century Europe*

Before the spread of printing press in Europe in the 1500s, information was highly scarce and relatively easy to control. For thousands of years until then, the scribal culture essentially handpicked the people who were given the code and tools to transmit knowledge across time and space (McLuhan M., 1962, p. 98). It was an economy of scarcity, ending up in intellectual starvation of the masses, as the book was perceived as a rare artifact, capable of containing knowledge sometimes sacred or even forbidden. The understanding of the empowering effect of such knowledge to a potential reader of a book often led the owner of the book to be very careful in allowing others to gain access to its content. Indeed, illustrations from the 16<sup>th</sup> century depict chained -even guarded- books, because of their secrets contained in their pages.

The printed book marks the beginning of the process of industrialization of information. Printing brought forth the potential and hope for abundance of information, threatening the control over knowledge due to scarcity. However, technological revolutions are not always accepted by society or by authority. Instances where the printed book was perceived as the work of the devil was not unusual. Daniel Dafoe (1727, p. 378) informs us of Gutenberg's partner Johann Fust ("Faustus") arriving in 15<sup>th</sup> century Paris with a wagon loaded with printed bibles. When the bibles were examined, and the exact similarity of each book was discovered, Fust was accused of black magic. Moreover and beyond reasons of religious disbelief, most emerging nation states of Europe considered printing a potentially revolutionary activity, and made it very clear that they would control information flow to their best of their ability (Johns A., 2010, p. 8). The printers were hunted down for printing forbidden documents, even more vigilantly than the authors of the texts. In this context, as printing technology developed, its pivotal social role became clear. It becomes associated with emancipation and the questioning of authority. With this in mind, William Berkeley, Governor of Virginia was writing to his overseers in England in the 1670s century saying "I thank God, there are no free schools nor printing (in Virginia); for learning has brought disobedience, and heresy (...) and printing has divulged them, and libels against the best government. God keep us from both" (Liehnhard, J., 1988).

Similarly, the basic idea of censorship in 18<sup>th</sup> century France is based on a concept of privilege, a license granted to a printer to publish a particular text that is denied to others. What was established was a centralized administration for controlling the book trade using essentially censorship and the monopoly of the established publishers. The state ascertained that the books, which were printed for distribution in their societies were authorized editions and within the control



of the state, the church or both (Pottinger D., 1958, p. 55 *et seq* Spinello R. & Bottis M., 2009).

Even so, this control was eventually incapable of controlling the spread of revolutionary thought. Parallel systems of distribution started to emerge as publishers and printing presses began to surround France, producing books which were smuggled across the French borders, distributed everywhere in the kingdom by an underground system (Danton R., 1996). Many of these book smugglers (or “pirates”) included prominent members of the Swiss or Dutch bourgeoisie merely acting on the basis of doing business and satisfying demand in the absence of an international system of copyright law; moreover, as this shadow trade was totally unregulated and affected only by the law of supply and demand, it is no wonder that most books contained political or pornographic material. As this expansion of the printing word takes over Europe and France, we note the emergence of a new reading public, not subject to the same norms of pre-approval and authorization.

## 2.2 *Origins of copyright in France and the UK*

It is in this context of censorship and control that the first regulatory attempts to control the flow of information are made by the Church (the first version of *Index Librum Prohibitorum* – a list of books prohibited by the Catholic Church – was promulgated by Pope Paul IV in 1559), the State, or both. Their attempts aimed to regulate and control the output of printers through censorship and accountability by introducing a system of privileges and by requiring printers to have official licenses to produce books. These licenses normally gave a printer the exclusive right, in the territory of the State where the license was granted, to print particular works for a fixed period of time (MacQueen H. *et al.*, 2007, p. 34).

This licensing mechanism operated in conjunction with two other devices: registers and patents. In England, for example, the printers and booksellers (called “Stationers” at the time) formed a guild, the “Stationers’ Company”, which in the 16<sup>th</sup> century was given the power to require the entry in its register of all lawfully printed books, which were printed entirely and exclusively by the guild’s members. A secondary purpose of such control was also to uphold the reputation of the craft community: conflicts over particular editions could be resolved by booksellers and printers by reference to these registers. In some cities, entries in registers became secure enough to act as *de facto* properties enduring throughout the 17<sup>th</sup> century (Johns A, 2010 p. 11). Indeed, the Licensing of the Press Act of 1662 provided that printing presses were not to be set up without notice to the Stationers’ Company, although it was originally limited to two years, and it was renewed until 1695 (Deazley R, 2006, p. 13).

Patents (in full “*letteraepatentes*”), on the other hand, were legal instruments in the form of an open letter (that is, which was both mailed to a person it addressed, and publicized so that all are made aware of it) from a ruler – as a royal prerogative - granting an office, right, monopoly or title to a beneficiary. In every respect, this kind of privilege was equivalent to the one granted for mechanical inventions, for newly imported crafts, or for a monopoly in a trade (Johns A., 2010, p. 11). With the advent of the printing press, they were sought to protect titles from unauthorized reprinting.

In pre-revolutionary France, royal privileges were exclusive and usually granted to the printers for six years, with the possibility of renewal (Dawson R., 1992, pp. 7-10). The French Booktrade and the “*Permission Simple*” of 1777 (Copyright and the Public Domain, 1992, pp. 7-10). Over time, it was gradually established that the owner of a royal privilege has the sole “right” to obtain a renewal indefinitely (Yu P., 2006, p. 141). Although initially the specific privileges were granted solely to the printers, in 1761 the Royal Council awarded a royal privilege to the heirs of an author rather than the author’s publisher, sparking a national debate on the nature of literary property. In 1777 a series of royal decrees reformed the royal privileges. The duration of privileges were set at a minimum duration of 10 years or the life of the author (whichever was longer). If the author obtained a privilege and did not transfer or sell it on, he could publish and sell copies of the book himself, and pass the privilege on to his heirs, who enjoyed an exclusive right into perpetuity (Dawson, 1992, pp. 7-10). If the privilege was sold to a publisher, the exclusive right would only last for the specified duration. The royal degrees prohibited the renewal of privileges, and once the privilege had expired anyone could obtain a “*permission simple*” to print or sell copies of the work. As a result, the public domain in books whose privilege had expired was expressly recognized (Yu, K., 2006, p. 141).

After the French Revolution, the National Assembly abolished the privileges. Anyone was allowed to establish a public theatre and the National Assembly declared that the works of any author who had died more than five years ago were public property. In the same scope, the National Assembly granted authors the exclusive right to authorize the public performance of their works during their lifetime, and extended that right to the authors’ heirs and assignees for five years after the author’s death. The National Assembly adopted the notion that a published work was by its nature a public property, and that an author’s rights are recognized as an exception to this principle, to compensate an author for his work (Yu, K., 2006, p. 141).

While the first copyright privilege in England was issued in 1518 for a term of two years, the first formal legal acknowledgement that there is a reason for con-

ferring exclusive rights to the creator of the work and not the printer of it, came with the passage of the Statute of Anne in 1709 in England. The statute was the first to recognize that legal rights derived from authorship, but it did not provide a coherent understanding of authorship or justification of authors' rights (Bainbridge D., 2006, p. 30). While the statute established the author as legal owner, and so provided the basis for the development of authors' copyright, it also provided a grandfather clause for the printers, allowing those works already published to enjoy twenty-one years of protection. Moreover, while an additional period of fourteen years was granted to the author, rather than the printer, the legislative intention of benefiting authors was undermined by practice. Given that the statute primarily intended to encourage public learning and to regulate the book trade, any benefits for authors in the statute seemed to be incidental. Furthermore, the primary foundation of the statute is a social *quid pro quo*: in order to encourage "learned men to compose and write useful books", the statute guaranteed a limited right to print and reprint those works and the creation of a public domain for literature.

Despite the recognition of a legal right directly to authors, many contracts between authors and publishers purported to assign the whole "right, title, property and interest" in the work to the publisher, and, towards the end of the eighteenth century, the courts treated such contracts as effective to transfer the reversionary term to the publisher, as for example in cases of *Millar and Dodsley v. Taylor* (1765) and *Carnan v. Bowles* (1785). Moreover, when the twenty-one years of the grandfather clause expired, the booksellers of London asked for an extension but the parliament declined to grant it, which prompted the booksellers to the courts, claiming that there was a natural right of copyright's ownership under the common law. The result was a decision of the House of Lords in *Donaldson v. Beckett* (1774), where the House denied the continued existence of a perpetual common law copyright and held that copyright was a creation of statute and could be limited in its duration. There was no common law copyright, and therefore no such common law right was impeached by the Statute of Anne.

Throughout the 18<sup>th</sup> century and particularly during the "booksellers' wars", an argumentation emerged whether copyright originated in author's rights to the product of his or her labor. This argumentation was further developed at the encouragement of the booksellers, not the authors, as this better suited their purposes and interests in convincing the authorities of the existence of a common law copyright. Thus, it was argued that the primary purpose of copyright was to protect authors' rights, not the policy goal of encouraging public learning (Lee, M., 2006, p. 13). As a result, and according to Patterson and Lindberg (1991), there a confusion remains about the nature of copyright ever since. Copyright has come to be viewed simultaneously from two contradicting perspectives; as a right

of the author based on natural law, as well as a statutory grant of a limited monopoly, based on the law and regulation of trade. What Patterson and Lindberg attest, however, is that proprietary authorship, while seemingly a natural right, emerged in fact by the late 17<sup>th</sup> and early 18<sup>th</sup> centuries because of the emergence of the London bookselling trade and because of the printing privileges granted to the booksellers.

Moreover, Locke's application of natural right theory in the domain labor advocated towards the need for protection of copyrighted works, in the form of commercialized ownership. The rights to the books were largely assigned to booksellers (Rose M., 1993). What emerged from the battle of the booksellers in the 18<sup>th</sup> century, however, was the concept of a "proprietary author", used as leverage in the struggle between London-based booksellers and the booksellers of the provinces. It is characteristic that in the case of *Donaldson v. Beckett*, the entire claim was made in the name of protecting the rights of the author, even though no author was actually involved in the case. In fact, as the counsel for the Scottish booksellers noted during the proceedings of the case "The booksellers (...) had not, till lately, ever concerned themselves about authors, but had generally confined the substance of their prayers to the legislature, to the security of their own property; nor would they probably have, of late years, introduced the authors as parties in their claims to the common law right of exclusively multiplying copies, had not they found it necessary to give a colourable face to their monopoly" (available at <http://www.copyrighthistory.com/donaldson.html#anm1>). Indeed, given that the primary beneficiaries of this new system of knowledge ownership were the booksellers (as the authors would assign their copyrights to them before publication), the concept of authorship simply created a useful euphemism for protecting their rights (Liang L. et al., 2005).

Finally, in order to tackle the problem of international enforcement for the protection of copyright works, caused by the exponential inter-state commerce of books and by the absence of an international mechanism to regulate and enforce copyright legislation, various States began to enter into negotiations for the mutual recognition and enforcement of foreigners' rights. This evolved in 1886 in the multi-national agreement known as the Berne Convention, for the protection of literary and artistic works.

### ***2.3 Impact on the development of copyright law in the United States – The Copyright Clause as an immigration incentive***

The Statute of Anne did not apply to the American colonies, as the colonies' economy was largely agrarian, and copyright law was not a priority, resulting in only three private copyright acts being passed in America prior to 1783. At the Constitutional Convention 1787, proposals were submitted that would allow Congress

the power to grant copyright for a limited time. These proposals are the origin of the “Copyright Clause” found in the US Constitution, which allows the granting of copyright and patents for a limited time “to promote the progress of science and useful arts”. The first federal copyright act, the Copyright Act of 1790 granted copyright for a term of “fourteen years from the time of recording the title thereof”, with a right of renewal for another fourteen years if the author survived until the end of the first term. With exception of the provision on protection of maps and charts, the Copyright Act of 1790 is copied almost verbatim from the Statute of Anne. Furthermore, in 1834, the Supreme Court ruled in *Wheaton v. Peters* (33 U.S. (Pet. 8) 591 (1834)), a case similar to *Donaldson v. Beckett*, that although the author of an unpublished work had a common law right to control the first publication of that work, the author did not have a common law right to control reproduction following the first publication of the work. The utilitarian function of the Copyright Clause of the US Constitution was further confirmed by the US Supreme Court in *Fox Film v. Doyal* 286 U.S. 123 (1932), where the court noted that “the sole interest of the United States and the primary object in conferring the (copyright) monopoly lie in the general benefits derived by the public from the labors of authors”.

Although printing greatly facilitated the propagation of literary and artistic works throughout Europe and over to the United States (which lead to the 19<sup>th</sup> century publishing battles between UK and US publishers), the same was not true for purely technical knowledge. We need to recognize that at the time of drafting of the US Constitution, the primary means of moving technological knowledge across the world was to move the brains that contained it (Moglen, E, 2007). The mere existence of printing did not bear a significant impact on this, particularly with regard to the communication of technological ideas. Indeed, before the appearance of the first volumes of the *Encyclopédie* in France (published between 1751 and 1772), there was no generally available source in the West providing technical knowledge to the public. The systematic representation and circulation of information concerning technology, enabling people to learn and educate themselves to produce for their benefit in a fashion productive of human self-realization and improved prosperity, is a much later idea.

In lack of generally available technical knowledge during that time, it is reasonable to consider that the British North Americans, living in an outpost of that western world at the end of the 18th century, blessed with what looked to them as a vast amount of empty land and a small number of skilled minds, desired vehemently to invite to the US skilled tradesmen, artisans, and those in possession of information in order to improve their agricultural production (Moglen E., 2007). This idea of encouraging skilled immigration as a development policy has already been conceived before the American revolution. The Dutch and English manor properties in New York and Pennsylvania, for example, were populated by

protestants from the part of Europe Louis the XIV destroyed in 1689, the Rhine Palatinate (Schulze L., 1996).

The great destruction of the Rhine Palatinate by Louis the XIV put in motion, along with his revocation of the edict of Nantes in 1685 (issued in 1598 and granted the Calvinist Protestants substantial civil rights in an otherwise very Catholic France) and the expulsion or enforceable conversion of protestants from France produced an enormous immigration of skilled tradesmen. As many as 400,000 Protestants chose to leave France, most moving to Great Britain, Prussia, the Dutch Republic, Switzerland, South Africa and the new colonies in North America (Morison S., 1972, pp. 220). In this sense, the Americans began their national experiment on top of an imperial experiment in the importation of skilled hands and minds as a primary economic development policy for their terrain. And to this purpose, the provision allowing the US Congress to pass laws that securing to writers and inventors exclusive rights to their writings and discoveries, for a limited time and for the better dissemination of science and the useful arts, is a provision to encourage skilled immigration to a land lacking intellect.

Moreover the argument of using copyright law as a migration incentive complies with the fundamental idea prevalent in US during that time, that monopoly as a form of royal prerogative and privilege is inherently intolerable, that government monopoly is a threat to freedom and a danger to constitutional propriety, because it offers an opportunity for the gaining of money outside the democratic dialogue of the republic, and it conceives of the idea of monopolization of new inventions for a limited time as an exception for the public good (Moglen E., 2007).

In the above context, it should be noted that what seems to be absent is the lack of the notion of intellectual property, as we came to know it today. There is no distinction between an idea and its expression within the Copyright Clause of the US Constitution. Nor a clear statement that ideas belong to the people who have them, because they made them, but only a limited exclusive right "*to promote the Progress and Science of useful Arts*". Indeed, the framers of the US Constitution were rather more likely than not to be learned in the literature of the 18<sup>th</sup> century and may have read *Tristram Shandy* (Sterne, L., 1759), in which Sterne wonders through his protagonist, when exactly does an idea becomes property of its thinker. By looking at Locke's example of the apple, Sterne goes on to note that the exudations of a man's brains are the same as the exudations of a man's breeches (Chapter 2.XXVII "That the sweat of a man's brows, and the exsudations of a man's brains, are as much a man's own property as the breeches upon his backside;-which said exsudations, &c. being dropp'd upon the said apple by the labour of finding it, and picking it up; and being moreover indissolubly wasted, and as indissolubly annex'd, by the picker up, to the thing pick'd up, carried home, roasted, peel'd, eaten, digested, and so

on;-'tis evident that the gatherer of the apple, in so doing, has mix'd up something which was his own, with the apple which was not his own, by which means he has acquired a property"). This parodic sense of a natural right in ideas appears to be common property of the people who wrote the US Constitution, and a consequence of a general distrust of monopolies. In this context, it seems the notion of intellectual property in the sense that we are now taught to perceive it as natural, is reflected in the Copyright Clause of the US Constitution, nor it is reflected in the agenda of 18<sup>th</sup> century publishers. In fact, it appears that the concept of ideas used in contemporary copyright law, is reflected exactly to the notion of the idea of 18<sup>th</sup>-century British empiricism; ideas are the external material to be used by the mind to create knowledge (Leiboff M., 2006). Ideas, experienced through the senses or the process of reflection based on observations of the material world, are the building blocks of knowledge.

In the light of the above, we note that the underlying concept in framing the Copyright Clause is overtly instrumental and utilitarian. There is a public value in the creation of an opportunity for rewarding those who think, as an exception from a general principle of social justice; the grant of monopolies by the State is wrong, and the only justifying purpose is to provide for social benefit through the creation of limited opportunities for the compensation of thinking, as a motivation for the European thinker to relocate across the Atlantic. In fact, one could recognize the same immigration incentives in the late 18<sup>th</sup> century copyright and patent law as the US Diversity Immigrant Visa Program of contemporary US law. -also known- the "Green Card Lottery", which makes available 50,000 permanent resident visas annually to persons from countries with low rates of immigration to the United States. And in this sense, if one wants to think of a working legal analog to U.S patent and copyright law made by late 18<sup>th</sup> century Congress, he might be inclined to consider the Green Card Lottery than the maximalist expansion of copyrights and patents during the 20<sup>th</sup> century, such as the patenting of genes, or the 90 years of copyright protection for works that belong to media conglomerates (Moglen E., 2007).

### **3. From the book to the record, to the film, to the VCR and beyond: the role of copyright in the 20th century processes of cultural production**

#### ***3.1 Copyright, the work for hire doctrine and the Fordist model of intellectual production***

From the world of printed book as the most popular artifact of commoditized information, we have moved over to the commercialization of electricity and spate of innovation occurring from the 3rd quarter of the 19<sup>th</sup> century to the end of

the 20<sup>th</sup>, into a world which is flooded with analog artifacts containing information. In this sense the book, is gradually accompanied, and eventually overrun by similar analog cultural artifacts, such as the moving picture, the sound recording, the cassette, the video-cassette, and other articles of available vernacular culture that put an immense amount of information not only at the disposal of the skilled reader but at the doorstep of everyone.

This commodification of information, unprecedented in its magnitude, should also be read in tandem with the great socio-economic changes that started to happen at the start of the 20<sup>th</sup> century, one of which was the rise of consumerism as a necessary trend to absorb the increase in the production output of western societies. Henry Ford's "conscriptio[n]" of the workers of the world into consumers signifies an explicit recognition that mass production was dependable on mass consumption (Harvey D., 1991, p. 126) and that this principle applies horizontally to the intellectual production output as well. Thus, Ford's five dollar, eight-hour work day served both to assure compliance with the discipline required to work the assembly line, but also to provide workers with sufficient income and leisure time to consume the mass-produced cultural artifacts produced by the corporate content providers (thus pausing the crisis of overproduction of commodities) (Harvey D., 2007, p. 195). However, in order to ensure the successful "conversion" of the workers into a new and reliable class of consumers, the new consumers had to acquire taste, needs and preferences, consumerism had to be indoctrinated. In Guy Debord's words, "waves of enthusiasm for particular products are propagated by all the communications media. A film sparks a fashion craze; a magazine publicizes night spots which in turn spin off different lines of products" (1967, p. 33). It follows that, the process by which the system of 20<sup>th</sup> century production learned to avoid the crisis, prophesized by the thinkers of the mid-19<sup>th</sup> century, relied on increasing dependence upon consumption fueled by media, which suggest, offer and recommend options for the consuming as well as the producing part of the system of economic relations.

It is in the above context that copyright becomes, through the work-for-hire doctrine and its relationship to the law of employment, the organizational prerequisite and facilitator for the creation of the 20<sup>th</sup> century media conglomerates. Once these have come into existence, then any new media that comes along has to be co-opted in the same way in order to maintain the principle of vertical integration. And as technology moved from publishing on paper to radio broadcasting, tv broadcasting, news dissemination, film dissemination, the same dominant model was applied; somebody makes an article of information, that act creates a property interest, that property interest is transferred through an employment contract and becomes a disposable piece of property in a market economy (Moglen E., 2007). The exceptions to this model, demonstrated by a number of "suc-



successful artists” who “have reached the top”, in fact help highlight the norm that the bulk of copyrighted work is owned by media corporations, record companies, movie studios e.tc. And as analog artifacts began to form this culture, which required industrial processes to produce books, records, films, tv shows e.tc., the ability of corporate content providers to control the means to produce these artifacts resulted in the ability to control how culture is produced and, more importantly, consumed. Control came naturally as part of the process of the existence of the medium itself (Moglen E., 2007). Indeed, as Mardsen (2005) notes, “the copyright industries have flourished due to the extremely rapid globalization of a few giants, whose control of vertical value chains from publishing to production to distribution to marketing on a massive scale have enabled total control of their industries”. In fact, in the 1920’s and 1930s, there was a sense that the progress towards centralized integrated models was somehow inevitable, simply the norm of industrial evolution. In the time of Henry Ford and other industrialists, it had seemed quite natural, in a Darwinian way, that the big fish ate the little ones until there were only big ones trying to eat one another (Wu T., 2010, p. 297). All the power would, thus, come to reside in few highly centralized giants, until some sort of sufficiently disruptive innovation came along and changed the game, allow small players to enter the market, and initiate the same Darwinian process of consolidation.

### ***3.2 Differences and similarities in 18th-20th copyright policy considerations***

In this sense, copyright law in the 20<sup>th</sup> century departs from its origins which justified its introduction in the 18<sup>th</sup> century, and it is used, through the wide-spread adoption of the work-for-hire doctrine, for encouraging the creation of larger, commercial publishing enterprises, which could in turn maintain control over cultural production. However, a differentiation between the 18<sup>th</sup> century printers and 20<sup>th</sup> century media conglomerates is apparent. In the age of the printing press, the introduction of copyright law aimed not only to ensure a return on the investment costs of the printers for the making of a printing press, but also aimed to incentivize the printers in selecting what to print based not only on market demand, but also on the nature of the work. It is at this point exactly where we think that there is a misconception with regard to the “incentive argumentation” evoked by the proponents of maximalist intellectual property laws, at least for the printers, producers and other facilitators of the production of cultural commodities. It is not as it has sometimes been suggested that if there weren’t incentives the producers wouldn’t print or produce anything at all. In fact, the 18<sup>th</sup> century printers built presses exactly because they knew that they were going to make money printing *something*. The question is whether what they ought to print is a classical work, somebody’s pornographic novel, or somebody’s political

treatise. In other words, the real question is how to determine what exactly will be created with the scarce industrial means and processes of production. In determining this question, usually the law of supply and demand plays a dominant role: Robert Danton noticed about 18th century French culture that what flowed into France from the presses of neighboring countries is what the French were not allowed to create for themselves, that is pornography and political treatises. As counter-balance to the law of supply and demand, copyright law attempted to give to printers a stake in the progress of literature so as to speed the diffusion of knowledge and the useful arts (Moglen E., 2007).

A similar incentive-oriented argumentation could in principle be said vis-à-vis the interests of the authors of the 18<sup>th</sup> century, but there is much historical evidence to suggest the opposite. The 19<sup>th</sup> century saw the prolific authorship of literary works in the absence of any meaningful protection afforded to authors by virtue of their copyright (Zimmerman D., 2003). While copyright protection existed, this protection rarely benefited the author beyond an initial payment for the copyright for their works (Liang L. *et al.*, 2005). This payment, often referred to as an *honorarium*, bore no relationship to the market value of the work, but was rather an acknowledgment of the writer's achievements (Woodmansee M., 1994, p. 42). In the majority of cases, most of the profits went to the publisher (Bainbridge D., 1999, p. 10) and, on occasion, authors were even asked to underwrite a portion of the publishing costs. It follows that in reality copyright protection usually benefited the publisher, and rarely the author (Calandrillo, S., 1998). This in fact explains the fervor with which the printers claimed the right of a perpetual common copyright law in the name of the authors, as indicated in the booksellers wars *supra*.

In light of the foregoing, we cannot unreservedly agree with the fundamental analytical proposition put forward by the defenders strong intellectual property laws in our time, as it seems to lack the historical and economical justification of the past two centuries. The claim that copyright laws should be strengthened, on the basis of a vague proposition that a natural right exists in favor of the author or publisher, does not go beyond mere mystification, and it fails to refute the historical findings, legislative and case law developments of the past two centuries. Furthermore, it fails to explain alienation, that is to say the separation of the intellectual worker from the fruits of his labor, based on the work-for-hire doctrine of the 20<sup>th</sup> century, particularly in the U.S legal configuration of the doctrine, where the employer's rights do not derive by the employee by an implied grant or assignment, but instead, they are deemed to be born directly in the name of the employer.

### ***3.3 Control as the cornerstone of copyright regulation at the start of the 21st century versus non-market based and decentralized models of cultural production***

At the end of the 20th century when we moved to a digital networked environment, the cultural information, contained exclusively in analog artifacts such as books, records or DVDS, begun to migrate towards the Internet, thus turning the cultural information, which was until then well controlled by its owners, into an attribute of the network itself. Consequently, the control that used to reside in the very making of these artifacts was jeopardized because of the inherent technological capability of the digital network to transfer information easily, immediately and without friction across the world. Moreover, and even more importantly, the enormous difference between the 20<sup>th</sup> and the 21<sup>st</sup> century brought by technological progress pertains to the ease of producing and sharing cultural information that the users create themselves, who are now capable of reaching out to the rest of the world. Whereas in the 20<sup>th</sup> century in the industrial model of cultural production the materials were produced by some set of professional commercial producers, who controlled the experience and located individuals at the passive receiving end of the cultural conversation, now with the technological advancements in computers and digital networks people can take more of their cultural environment, more of the information environment, make it their own, use it as found materials to put together their own expressions, do their own research, create their own communications and collaborate with others rather than relying on a limited set of existing institutions or on a set of materials that they are not allowed to use without permission (Benkler Y., 2007). This is the essential difference from a world of the catholic churches control of ideas threatened by the “protestant” book to a world in which the media conglomerates benefited from control over books, celluloid, vinyl e.tc. and the scarce and expensive means to produce it, and eventually to a world in which the technology makes production and sharing of cultural information as easy as their consumption (Moglen E., 2007). Through the democratizing effect of technology, we are witnessing an unprecedented increase in user autonomy, namely the ability of people to do more for themselves and by themselves, without having to submit to anyone’s control or ask for their permission (Benkler Y., 2006, pp. 8, 133).

As the ease and immediacy of frictionless sharing of cultural information jeopardized control over the consumption of cultural goods produced by media conglomerates, the economic foundations of cultural production of 20<sup>th</sup> century began to crack. Resisting this transition was an inevitable step, as the new capabilities of technology were perceived as a threat by the corporate content providers. In order to force technology into compliance with the 20<sup>th</sup> century industrial mode of production, copyright laws were updated with a view to regain control. Al-

though, technology facilitated the jointure between the user, consumer, producer and distributor of cultural content, the law intervened to force a differentiation of roles once more. The Digital Millennium Copyright Act in the USA and the Copyright Directive (2001/29/EC) in the EU were just two legislative examples, that incorporated provisions regarding control over use, not just control over production and organizational dispositions, as it was the case with 20<sup>th</sup> century law making. Hollywood's campaign to expand technological constraint by backing Digital Rights Management systems (pejoratively called by its opponents "Digital Restrictions Management") and Technological Protection Measures for the use of digital media and products, as well as condemning peer-to-peer technologies are some examples of 20<sup>th</sup> century owners of cultural production to impede the gradual loss of control, as tangible cultural artifacts become bits over the network and then are shared by users all over the world.

Particularly with regard to law making, it is interesting to briefly note a number of legislative preferences adopted in international treaties and/or national legislation, which indicate a general disposition of the legislators in favor of proprietary models of cultural production, increased control over the cultural goods and rent-extraction by industrial producers:

1. Introduction of Digital Rights Management technologies: DRM architectures can be arguably described as an aggregation of security technologies to protect and enforce the interests of the content providers, so that the latter may maintain a persistent control over their content. In particular, a DRM system specifies, manages, and enforces rules (that is, the content providers' rules), focusing mostly on the usage and distribution of their information products. It follows that a sophisticated DRM system involves not only the mere granting of access to specific information, but also the processing of all kinds of information for the electronic administration of rights in order to ultimately enable end to end rights management throughout the value chain (WIPO, 2004, p. 11). The use of such systems enables very granular control of the content and, therefore, allows content owners to apply various usage models or even introduce new marketing strategies (e.g. pay-per-access).

2. The emergence of a new form of license pertaining to the "right to read". As prominent copyright law expert Jessica Litman observed (1994, p. 29), the basic right of copyright, to control copying, was never seen to include the right to control who reads an existing copy, when, and how many times. As however, cultural commodities became digitized, and considering that accessing a work in a digital format requires the creation of a temporary copy in the Random Access Memory of a computer device, the formal rights of copyright holders were expanded to cover any and all computer-mediated access to their works. More

importantly, combined with the possibility and existence of DRMs and technological protection measures to establish control and the law's prohibition to circumvent said controls (even in cases of legitimate copyright exceptions or fair use), the law extends an iron grip on how cultural goods are accessed and used.

3. Criminalization of non-commercial infringing activities: Criminal liability has been expanded to cover non-commercial activities which according to the law are considered illegal, including free sharing of copyrighted materials. While it is one thing when the recording or movie industry calls millions of users of P2P networks "pirates" in a rhetorical stunt to conform social norms to their established business model, it is completely different when the state itself outlaws, fines and threatens with imprisonment such a significant portion of society (Benkler Y., 2007, p. 442).

4. Constant increase in the term of protection for copyrighted works The most recent retrospective extensions (to a term already stretched numerous times over the past century and which already offered 99% of the value of a perpetual copyright) had the practical effect of helping a tiny number of works (between 1% and 4% (Boyle J., 2004). As a result in order to ensure that control to this handful of works is maintained, the public is denied access to the remaining 96% of the works that would otherwise pass into the public domain, thus depriving the poor and intellectually starving minds of the world from access to educational and cultural materials which could be distributed at virtually no cost. The "loss" caused by copyright here rivals and exceeds any possible loss from "piracy" (Boyle J., 2004).

The aims of the content industries in the 20<sup>th</sup> century, which lobby heavily for a constant expansion and stricter enforcement of existing copyright laws, is well understood; if the same model of control through a centralized industrial production could be maintained and legally enforced as our cultural production becomes digitized, the new era should be able to produce for the privileged owners of the 20<sup>th</sup> century a state of grace. As "all that is solid" melts into bits and bytes, the owners would still be able to charge for digital distribution of cultural goods, the traditional business model of cultural production could still be maintained, if not improved, since now the producers would continue to get paid for digital artifacts that they have no marginal cost. However, the challenge now relies in the very social behavior of the public and its primal urge to communicate through sharing. In the words of Yochai Benkler (2007) "one can always try to create artificial boundaries, technological boundaries, which could prevent people from sharing files, music, e.t.c. But how can somebody create a wall or a boundary against the very basic desire of sharing. One basic reason why the war on piracy is failing is social: people like to communicate, people like to share things and

transform them, and technology makes it so easy that there's no apparent way of stopping it".

The technological developments of the 21<sup>st</sup> century, particularly those of information processing, storage and communication, have made non-proprietary and non-centralized models of cultural production more attractive and effective than was ever before possible. Ubiquitous low-cost processors, storage media and networked connectivity have made it practically feasible for individuals, alone and in cooperation with others, to create and exchange information, knowledge, and culture in patterns of social reciprocity, redistribution, and sharing, rather than proprietary market-based production (Benkler Y., 2006, p. 462). These technological conditions have given individuals a new practical freedom of action, and an unprecedented opportunity to create and distribute cultural information with the rest of the globe, without the necessity to resort to the owners of the cultural means of production of the 18<sup>th</sup>, 19<sup>th</sup> and 20<sup>th</sup> century for financing their projects. Market-based production is now accompanied by an emerging possibility of producing and sharing cultural information through non-market models, containing the intellectual production of individuals either acting alone or in cooperation with each other.

In this context, the emergence of the possibility to create, share and distribute information goods should be read in line with the equally emergent phenomenon of peer production. Successes such as the free and open source software movement and that of the Wikipedia challenge the conventional thinking about economics of information production, as they diminish the role of proprietary/closed markets and hierarchically organized firms. Although this sort of social production and exchange was always present in our societies, its role was largely undermined by the industrial model of market production, mostly because the creation and distribution of analog artifacts still required high capital costs (a printing press, a music studio, e.tc.). Now, however, as technological progress minimized the costs of creating and moving information on the Internet, peer production appears as rational and efficient at the turn of the 21<sup>st</sup> century, similar to Ford's assembly line was at the beginning of the 20<sup>th</sup> century, and the pooling of human creativity (or even computation, communication and storage) enables non-market incentives and relations to play a much larger role in the production of the information environment than it has been able to in the past (Benkler Y., 2006, p. 470).

#### **4. Balancing copyright objectives with different models of cultural production**

In this paper, we have attempted to identify the interrelation between copyright and industry regulation, the cause and effect of copyright policies on the behavior

of market and social actors throughout the past centuries as well as the contribution of copyright law as a regulatory factor of economic relations. We started by examining the social conditions during the introduction and spread of the book as the first mass-produced cultural article in western civilization, and the policy decisions taken with regard to the regulation of an emerging market which was created by the growing demand of the public. We attempted to show the dominant role of the printers and booksellers in this growing market -a role far more dominant than that of the authors- and their attempts to preserve their monopolies and privileges in retaining exclusive control over the way books are produced and marketed by evoking the theory of a natural right of the author to own the fruit of intellectual labor, a theory however which, not only does not seem to be confirmed by the historical and social trends of the time, but also it seems to be undermined whenever the rights of the authors are in conflict with the rights of the printers, producers of records, and other owners of the means of intellectual production until the 20<sup>th</sup> century.

For this purpose, we have looked at the wide-spread adoption of the work-for-hire doctrine in 20<sup>th</sup> century intellectual production, and how the relationship of copyright with employment law helped create large, centralized models of production, which created polished cultural goods for consumption by the rising class of workers. We justified the creation of large media conglomerates which owned the vast majority of cultural production to this factor, which continued to grow by leveraging their control over the scarce and expensive means of production. Finally, we attempted to describe how the technological changes at the end of the 20<sup>th</sup> century were treated as a threat to the 20<sup>th</sup> century model of centralized market-based cultural production, and we noticed that maximalist rhetoric in favor of stronger protection and enforcement of intellectual property rights, a rhetoric which has already been followed to some extent by legislators around the globe.

We are currently observing a steady trend in copyright law, but a growing counter-trend in societal behavior. In law, we are witnessing a continual strengthening of the control that the owners of intellectual property rights are allowed to exert. These changes tip the balance in favor of business models and industrial production practices that are based on exclusive proprietary claims which limit the public sphere, in an era where people who cannot afford to buy information goods may enjoy unprecedented possibilities to access it at virtually no cost; it is no wonder that the biggest advocates of these changes are the media conglomerates of the 20<sup>th</sup> century, which collect large rents if these laws are expanded and enforced. Social trends, on the other hand, are pushing in the opposite direction following the trends of a networked information economy, of non-market production, of an increased sharing mentality, and of an increased ambition to par-

ticipate in communities of practice that produce information, culture and knowledge for free use, re-use and sharing of such information by others (Benkler Y., 2006, p. 470). These new patterns of social cultural production bring with them the possibility of increased social surplus, but they are also bound to destabilize the status quo of established market-based production models, likely resulting in significant redistribution of wealth and power from previously dominant firms not only to social groups, but also to a number of businesses that will decide to reconsider their business models and build tools and platforms to accommodate the newly productive social relations.

What lies at the core of this tension is, in our view, a dispute regarding the legitimacy of the emerging new model of non-market decentralized production, and the extent to which this model may be allowed to use, share and re-use cultural goods in light of the utilitarian and instrumental origins of copyright legislation. In this debate, based on the aforementioned findings, we believe that any argumentation that conceals itself behind a rhetoric of a theory on natural rights of the authors would be irrelevant, if not misleading. It would be much more helpful to focus on how to ensure the positive potential and promise that lies in today's means of creating and sharing cultural goods and to recognize a more nuanced understanding of the public sphere, with the presumption being that the author is not a figure who has to be protected from this public sphere but one who resides and works within it (Liang *et al.*, 2005)

## References

Bainbridge, D. (1999), Cases and materials in intellectual property Law, 2<sup>nd</sup> ed., Financial Times Management.

Bainbridge, D. (2006), Intellectual property, 5<sup>th</sup> ed., Pearson Education.

Benkler, Y. (2007), On autonomy, control and cultural Experience, (interview) online at <<http://footage.stealthisfilm.com/video/5>>.

Benkler, Y. (2006), The wealth of networks, Yale University Press.

Boyle, J. (2004), A Manifesto on WIPO and the Future of Intellectual Property, Duke Law & Technology Review No. 9, online at <<http://www.law.duke.edu/journals/dltr/articles/PDF/2004DLTR0009.pdf>>.

Calandrillo, S. (1998), An economic analysis of intellectual property rights: justifications and problems of exclusive rights, incentives to generate information, and the alternatives of a government-run reward system, Fordham Intellectual Property, Media and Entertainment Law Journal, p. 301 *et seq.*



Danton, R. (1996), *The forbidden best-sellers of pre-revolutionary France*, Norton, W. W. & Company.

Dawson, R. (1992), *The French Booktrade and the "Permission Simple" of 1777: Copyright and the Public Domain*, Voltaire Foundation.

Deazley, R. (2006), *Rethinking copyright: history, theory, language*, Elgar Publishing.

Debord, G. (1967), *The society of the spectacle*, Rebel Press.

Defoe, D. (1727), *The history of the devil as well ancient as modern: in two parts*, 2<sup>nd</sup> ed., London.

Johns, A., (2010) *Piracy: the intellectual property wars from Gutenberg to Gates*, University of Chicago Press.

Harmon, A. (2002), Black hawk download: moving beyond music, pirates use new tools to turn the net into an illicit video club, *New York Times*, January 17.

Harvey, D. (1991), *The condition of postmodernity: an enquiry into the origins of cultural change*, Wiley-Blackwell.

Harvey, D. (2007), *The limits to capital*, Verso.

Lakoff G., and Johnson, M. (1980), *Metaphors we live by*, University of Chicago Press.

Lee, M. (2006), *Bootlegging: romanticism and copyright in the music industry*, Sage.

Lessig, L. (2008), *Remix: making art and commerce thrive in the hybrid economy*, Penguin Press.

Liang, L., Mazmdar A., and Suresh M. (2005), *Copyright/copyleft: myths about copyright*, online at <<http://www.countercurrents.org/hr-suresh010205.htm>>.

Liehnhard, J. (1988), *Printing in williamsburg*, University of Houston, online at <<http://www.uh.edu/engines/epi924.htm>>.

Litman, J. (1994), *The exclusive right to read*, *Cardozo Arts and Entertainment Law Journal*, Vol. 13, 29.

Leiboff, M. (2006), *Tristram Shandy and the limits of copyright law*, online at <[http://www.law.unimelb.edu.au/cmcl/seminars/Marett%20Leiboff%20Passages\\_paper\\_format\\_final.pdf](http://www.law.unimelb.edu.au/cmcl/seminars/Marett%20Leiboff%20Passages_paper_format_final.pdf)>.

MacQueen, H., Waelde, Ch., Laurie, Gr. (2007), *Contemporary intellectual property: law and policy*, Oxford University Press.

McLuhan, M., (1962), *The Gutenberg galaxy: the making of typographic man*, University of Toronto Press.

Marsden, Ch. (2005), *Free, open or closed – approaches to the information ecology*, Emerald Group Publishing Limited.

Moglen, E. (2007), *From the birth of printing to industrial culture; the root of copyright* (interview), online at <<http://footage.stealthisfilm.com/video/10>>.

Morison, E. (1972), *The oxford history of the American people*, New York City: Mentor.

Patterson, L, Lindberg, S. (1991), *The nature of copyright: a law of users' rights*, University of Georgia Press.

Pottinger, D. (1958), *The french book trade in the ancien regime, 1500 - 1791*, Harvard University Press.

Rose, M. (1993), *The invention of copyright*, Harvard University Press, 1993.

Schulze, L. (1996), *Irish palatine story on the Internet*, in *Irish Palatine Association Journal*, No. 7 December 1996, available at <<http://www.olivetreegenealogy.com/palatines/palatine-history.shtml>>.

Spinello, R. & Bottis, M., *A defense of Intellectual Property Rights*, 2009, Edward Elgar Publishing.

Sterne, L. (1757), *The life and opinions of Tristram Shandy*, Gentleman.

Weber, H. (1996), *Paper bullets: print and kingship under Charles II*, University Press of Kentucky.

WIPO Standing Committee on Copyright and Related Rights (2004), *Current Developments in the Field of Digital Rights Management*, SCCR/10/2, available at <[http://www.wipo.int/edocs/mdocs/copyright/en/sccr\\_10/sccr\\_10\\_2\\_rev.pdf](http://www.wipo.int/edocs/mdocs/copyright/en/sccr_10/sccr_10_2_rev.pdf)>.

Woodmansee, M. (1994) *The author, art, and the market*, Columbia University Press.

Wu, T. (2010), *The master switch*, Random House.

Yu, K. (2006), *Intellectual property and information wealth: issues and practices in the digital age*, Praeger Perspectives.

Zimmerman, D. (2003) *Authorship without ownership: reconsidering incentives in a digital age*, NYU Law School, Public Law Research Paper No. 55, online at SSRN: <<http://ssrn.com/abstract=38252>>.

# **Mobile devices, virtual presence, and surveillance: questions concerning epistemology and some new challenges for privacy and data protection**

---

---

**Karsten Weber**

---

---

## **Surveillance and Control**

Since several years, surveillance and control is a pretty hot topic in scholarly as well as in political debates. To some extent, the 9/11 incident gave birth to these discussions and debates, at least on the political level. However, research on issues of surveillance and control in modern or, as some would say, postmodern societies began much earlier than 9/11. In many respects, one could say that Michel Foucault started this kind of research with the publication of his book “*Surveiller et Punir. La Naissance de la Prison*” in 1975. And if one takes the scholarly debates concerning privacy into account, one might say that research on surveillance and control started much earlier, for instance with Samuel D. Warren and Louis Brandeis’ hallmark paper “The right to privacy”, published in 1890.

A large part of this ongoing debates deal with the relation of the state and its citizens. According to Foucault and many other scholars, surveillance and control are methods to govern people. From this point of view, surveillance and control are understood as something repressive, as methods to force people to do things they otherwise would not do. Other scholars like David Lyon (2007) stress that surveillance and control make possible social sorting which means that certain people at certain places are labelled as “[...] ‘undesirables’ by examining individuals’ immediate attributes for disliked characteristics. A person might fall into a pariah category because of what she is wearing, who she is “hanging out” with, or her demographic category”, as Kang and Cuff (2005: 122) puts it.

Common understanding of surveillance and control most frequently implies that there is some kind of Orwellian ‘Big Brother’ who is watching us. Regularly, state authorities like the police or secret services are identified as Big Brothers, but insurance companies, search engine providers like Google and companies running social networks like Facebook – generally speaking private companies – are also very often mentioned. These actors collect, process, and store huge amounts of personal related information and use it in their own interest. Compared to them, we as citizens or consumers are relatively powerless.

## Sousveillance and Equiveillance

To abate or even abolish this asymmetric power relation, Steve Mann (2004b: 620) suggests that people should employ information and communication technology for the purpose of ‘sousveillance’ which “[...] refers both to hierarchical sousveillance, e.g. citizens photographing police, shoppers photographing shopkeepers, and taxi-cab passengers photographing cab drivers, as well as personal sousveillance (bringing cameras from the lamp posts and ceilings down to eye-level, for human-centered recording of personal experience).” Additionally, Mann, Fung, and Lo (2006: 177) coined the term ‘equiveillance’ to emphasize “[...] a peer-to-peer approach that decentralizes observation to produce transparency in all directions.”



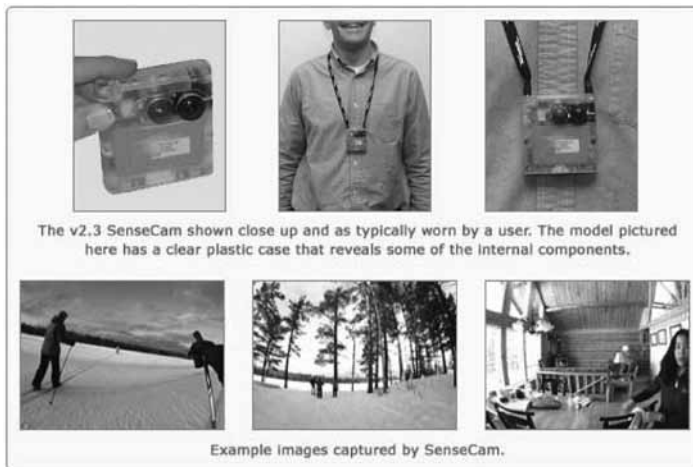
**Figure 1.** Evolution of cyborglogging (Mann 2004a: 4).

Briefly speaking, sousveillance and equiveillance are characterized by two aspects. The first one must be understood in a political sense, as already pointed out: Sousveillance and equiveillance shall wane or eliminate an asymmetry of power between, for example, state authorities and citizens. Each and every citizen shall be empowered to employ the same surveillance measurements as state authorities and companies do. The second aspect must be understood in more individual as well as social terms: Mann and his colleagues would like to use technology for artistic reasons to create some kind of multimedia diaries – called ‘cyborglog’ as well as for purposes concerning social interaction.

They demonstrate that ordinary mobile phones can be employed for cyborglogging or ‘glogging’. In principle, they created a client-server-architecture with mobile phones as clients with which pictures can be taken and text can be entered. Pictures and text are sent in real-time to a server on which they are stored. Users of these servers now can access those contents using a web browser in real-time, too. The authors stress (Man, Fung, Lo 2006: 178) that “[in] contrast to other

photosharing sites, where images are uploaded from PCs, 'glogger uses camera phones which are commonly carried by people in their day to day lives in real-time." A Microsoft Research project called "SenseCam" (<<http://research.microsoft.com/en-us/um/cambridge/projects/sensecam/>>, last visited 2011/04/22) realizes a somehow similar approach although in this case no automatic transmission of photos to a website takes place; instead the photos are stored within the camera.

Mann, Fung, and Lo also discuss the social, moral, and legal aspects of the technology they developed. With regard to the paper at hand, one of the most important aspects they bring up is that the cyborglogging system as well creates an asymmetric power relation although it was supposed to mitigate such asymmetries. This accrues from the fact that only the person who wears and utilizes the mobile phone actually knows whether it takes pictures or not. This raises moral and legal concern, as Mann, Fung, and Lo (2006: 179) admit: "Naturally, as with any new technology, there will be both advocates as well as opposers. When faced with the moral or ethical dilemma of when to run 'glogger, we consider, as a base-level of operation, the notion of *equivoillance*. *Equivoillance* doctrine says that as long as surveillance is present in the environment, that a person ought to have a moral and ethical right to engage in *sousveillance*."



**Figure 2.** Microsoft SenseCam.

From the point of view of an ethicist it must be stressed that Mann, Fung, and Lo's position seems to be somehow naïve and therefore must be challenged. For the presence or absence of a moral right does not depend on whether others act according equivalent moral rules. To exaggerate a bit but bring it to the point:

one does not have the right to misbehave just because there are people who behave in a morally wrong way. Additionally, it has to be stressed that in some countries, for instance, Germany, under certain circumstances it is legally prohibited to take pictures of persons without their informed consent (§823 BGB; §201a StGB; §§22-24, 33, 37, 38, 42-44, 48, 50 KUG). But although these moral and legal aspects are most interesting as well as important, here they shall not be examined anymore.

## **Mobile Phones and Real-Time Video Streaming**

In earlier papers (e.g. Mann 2004a), Steve Mann already brought up the idea of “continuous lifelong capture of personal experience” using video technology. Other scholars mentioned technologies that could be employed to share experiences and to communicate and interact across the borders of spatially separated environments (cf. Brown et al. 2003; Nijholt, Zwiers, Peciva 2007). These ideas and conceptions now shall be put a step further. Let’s suppose the following scenario: K. is carrying a Bluetooth headset equipped with a microphone, earphones, and a small head mounted camera. Compared to Mann, Fung, and Lo’s setting this would assure that the camera would have almost exactly the same perspective as the person carrying it. A modified version of the technical infrastructure that Mann and his collaborators presented might be used to transmit and receive video streams in real-time from one 3G mobile device to another or even to a couple of them. Received video streams may be projected on any suitable surface employing a micro beamer. Another option would be to utilize a Tablet PC to show video streams and to transmit own content. A bit more high-tech would be to use head mounted displays.

A first or simple version of this technology would merely transmit video streams and the respective sound; however, it certainly would be possible to augment the visual and acoustic channel with other sensory input, for instance, from haptic interfaces, or data concerning environmental conditions such as temperature or humidity. It might also be useful to transmit data about the physiological conditions of users. Yet, it would be (rather) easy to monitor heart beat frequency, blood pressure, and the like, but it would be much more difficult to bring these data to the attention of the receiving person in an adequate and effective way: just showing numbers on a display would not provide for a real experience.



**Figure 3.** A mobile phone as wearable device (Mann, Fung, Lo 2006: 179).

In some situations it might be very useful to record all the above mentioned information in order to evaluate and review them later on, for instance, in case of emergency rescue, law enforcement, or even combat missions. However, this kind of usage shall not be discussed further. Instead, the real-time application of such technology shall be evaluated.

Although persons using this setting might be spatially separated by huge distances, for them it would be possible to interact with each other in a pretty new way: they would hear and see what their peers would hear and see and vice versa. In fact, one could say that, although a person not really resides at a place, she is present. This concept shall be called 'virtual presence'. The difference resulting from comparison of (this) "virtual" presence" with 'telepresence' or 'copresence' is that these (techniques) generally require using video-conferencing equipment that they are virtually present" is located in a room designated just for this" (cf. Pinhanez, Pingali 2004). Moreover, at least the simplest technical solutions of virtual presence would utilize already existing consumer products. However, it must be stressed "that one must focus or not so much the technology itself as on its epistemological consequences".

### **A New Understanding of Presence**

It is obvious that a technology like virtual presence would raise make moral and legal questions just as pressing as the original concept of Mann, Fung, and Lo,

particularly with regard to surveillance and control, privacy and data protection. It has to be stressed that the new setting would not abolish the asymmetric power relation between the person employing virtual presence and those who are pictured as long as no additional technological measurements are utilized or respective social rules are enforced. However, such aspects shall not be discussed any further in the paper at hand. Rather, the epistemological consequences of virtual presence shall be evaluated.

The major appeal of virtual presence surely would be that in principle we would be able to communicate and to interact with persons spread across spatially separated environments all over the world; we could 'attend' any event anytime anywhere. But as the famous Science Fiction writer Isaac Asimov already described in 1957 in his novel "The Naked Sun", our understanding of being present might change dramatically: 'to be present' and 'to reside' then would mean something completely different. Furthermore, virtual presence might change our understanding of reality, particularly if high-tech equipment, as mentioned above, would be utilized.

Indeed, the idea that a mind-independent reality does not exist is widespread among social scientists and philosophers (e.g. Berger, Luckmann 1966). But even if one sticks to the idea that there is a mind-independent reality, most scholars would agree that to a certain extent our experience of reality is a theory-driven creation, construction, or fabrication of our brain determined by our knowledge, prejudice, and expectations. What we, for instance, see is not something like a representation of the world as it is rather an image that, to a large extent, our brain creates. Moreover, it is widely accepted among most scholars that media of any kind strongly influence the process of constructing a worldview. Therefore, since virtual presence is a kind of media, it would affect our worldview, too. But the totality of virtual presence seems to introduce a leap in quality, if compared to other media like broadcasting or television. If anything, the experience of virtual presence might only be weighed against the total immersion that can take place while playing computer games or going through virtual realities (cf. Cranny-Francis 2007).

One other difference compared to media like broadcasting or television is that it would not make sense anymore to talk about content of (digital) media. For this content will be integrated in our own experience in such a way that one cannot talk about a representation or mapping of reality (cf. May, Hearn 2005: 200). Hence, at least to some extent, the dualism of I and world might be abrogated because the distinction of world on the one hand and information or knowledge about the world on the other hand could not be drawn anymore. Virtual presence just might taken for granted the same way like today the possibility to talk with



others from distance via mobile phone. Current findings already suggest that using mobile phones shows deep impacts to psychological traits of their users (Perriera 2005; García-Montes, Caballero-Muñoz, Pérez-Álvarez 2006). At least it can be stated that virtual presence probably would blur the borders of virtual and embodied or physical space and would help to create what often is called 'hybrid space' (e.g. de Souza e Silva 2006).

## Truth and Falsity of Images

In his famous novel "1984" George Orwell not only described a society characterized by ubiquitous surveillance and control but he also depicted the methods of historical misrepresentation by manipulation of documents of any kind. One of these methods is photomontage. In our times we know the verb 'to photoshop': its use shall indicate that a digital picture was modified to increase, for instance, its quality. But pictures can be manipulated to the extent that they do not depict the truth show anymore.

It is attractive seductive to believe that as long as we know all steps of the production and reproduction of a picture – or any other kind of document that shall represent reality – we should be able to authenticate the validity of this particular picture. But even if we assume that a picture actually can represent reality, we have to learn that the validity of a picture must be authenticated not only by technical means but by socially defined rules. As observers we must rely on the pres.... that a picture shows reality as it is. In this regard, Escudero Chauvel (1997) coined the term 'media contract' for the rules which shall authenticate the validity of documents that shall represent reality. In case of, traditional journalism for instance, one might say that this media contract actually performs more or less successfully. But one should be skeptical whether equivalent rules can be defined, implemented, and enforced in the case of virtual presence.

For one has to learn that virtual presence will probably come together with the disposability of huge computing capacities on the server's side as well as on the client's side. It has been already five or six years that mobile devices provide for computing capacities that are comparable to those of personal computers. The respective computing power would suffice to employ at least simple real-time video manipulation and filtering. Moreover, on the server side cloud computing can provide for pretty cheap and massive computing capacities. These can be utilized to manipulate transmitted pictures and video streams in real-time or with minute delays only. For the recipients of such content it would be very difficult or even unfeasible to determine whether it is authentic or manipulated.

Hence, from the point of view of epistemology it might be still possible to determine what is real and what is a construction based on technology. But reason-

ably, one might be skeptical whether we, as users of virtual presence, would be able to decide if the transmitted information is authentic or manipulated.

## Further Research

As previously pointed out, technologies like virtual presence raise serious moral and legal questions concerning privacy, data protection, power relations, and the like which that could not have been discussed in the paper at hand. To answer those questions, at first it would be necessary to clarify which moral and legal norms and rules would be affected by virtual presence. Additionally, it would be mandatory to evaluate users' expectations, hopes, fears, and of course reactions with regard to such a technology because it would not make sense to be concerned about virtual presence if its potential users would decline to apply it.

Furthermore, bandwidth available for consumers using mobile devices would allow for services that would not merely only employ visual and acoustic channels for communication and interaction. Technology could provide for other sensory input applying, for instance, haptic interfaces. Therefore, it would be essential to empirically evaluate which interfaces in which situations and for which use cases would be most appropriate for interaction across spatially separated environments.

## Conclusion

Mann, Fung, and Lo's conception of technology that makes feasible sousveillance and eavesdropping was presented to show that ubiquitous computing technology not necessarily supports surveillance and control in an Orwellian sense. Virtual presence as a modification and extension of the cyborglogging design was introduced to support communication and interaction of persons residing in spatially separated environments. It was demonstrated that without further technological means or respective social rules the new setting raises the same moral and legal concern as Mann, Fung, and Lo's design. Moreover, it was talked about epistemological theories of reality and that our understanding of presence would substantially change if virtual presence would be employed. Finally, it was stressed that users of virtual presence probably will not be able to determine whether that what they experience could be an authentic or manipulated reproduction of reality.

## References

- Berger, Peter L., Luckmann, Thomas (1966): *The Social Construction of Reality. A Treatise in the Sociology of Knowledge*. New York: Random House.
- Brown, Barry, MacColl, Ian, Chalmers, Matthew & Galani, Areti; Randell, Cliff; Steed, Anthony (2003): *Lessons from the Lighthouse: Collaboration in a Shared*

*Mixed Reality System*. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Fort Lauderdale: ACM, 577-584.

Cranny-Francis, Anne (2007) *Ecce Techno, or, Suiting the Biomechanical Platform: Immersion and Contemporary Embodiment*. In: Visual Communication 6 (2): 156-169.

de Souza e Silva, Adriana (2006) *From Cyber to Hybrid: Mobile Technologies as Interfaces of Hybrid Spaces*. In: Space and Culture 9 (3): 261-278.

Escudero Chauvel, Lucrecia (1997) *The Media Contract*. In: Nöth, Winfried (ed.): Semiotics of the Media. State of the Art, Projects, and Perspectives. Berlin, New York: de Gruyter, 99-107.

Foucault, Michel (1995) *Surveiller et Punir. La Naissance de la Prison*. Paris: Editions Gallimard.

García-Montes, José M., Caballero-Muñoz, Domingo, Pérez-Álvarez, Marino (2006) *Changes in the self resulting from the use of mobile phones*. In: Media, Culture & Society 28 (1): 67-82.

Kang, Jeffrey, Cuff, Dana (2005), *Pervasive Computing: Embedding the Public Sphere*. In: Washington & Lee Law Review 62: 93-146.

Lyon, David (2007), *Surveillance, Security and Social Sorting: Emerging Research Priorities*. In: International Criminal Justice Review 17 (3): 161-170.

Mann, Steve (2004a), *Continuous Lifelong Capture of Personal Experience with Eye-Tap*. In: Proceedings of the 1<sup>st</sup> ACM Workshop on Continuous Archival and Retrieval of Personal Experiences. ACM: 1-21.

Mann, Steve (2004b), *"Sousveillance": Inverse Surveillance in Multimedia Imaging*. In: Proceedings of the 12<sup>th</sup> Annual ACM International Conference on Multimedia. New York: ACM, 620-627.

Mann, Steve, Fung, James, Lo, Raymond (2006) *Cyborglogging with Camera Phones: Steps toward Equiveillance*. In: Proceedings of the 14<sup>th</sup> Annual ACM International Conference on Multimedia. Santa Barbara: ACM, 177-180.

May, Harvey, Hearn, Greg (2005) *The Mobile Phone as Media*. In: International Journal of Cultural Studies 8 (2): 195-211.

Nijholt, Anton; Zwiers, Job; Peciva, Jan (2007) *Mixed Reality Participants in Smart Meeting Rooms and Smart Home Environments*. In: Personal and Ubiquitous Computing 13 (1): 85-94.

Pertierra, Raul (2005) *Mobile phones, identity and discursive intimacy*. In: Human Technology. An Interdisciplinary Journal on Humans in ICT Environments 11: 23-44.

Pinhanez, Claudio, Pingali, Gopal (2004) *Projector-camera systems for telepresence*. In: Proceedings of the 2004 ACM SIGMM Workshop on Effective Telepresence. New York: ACM, 63-66.

Warren, Samuel & Brandeis, Louis D. (1890) *The Right to Privacy*. In: Harvard Law Review 4 (5): 193-220.

# **Information technology, millennials and privacy: can they blend or will they collide?**

---

---

**Aharon Yadin**

---

---

## **1. Introduction**

The rapid advancement in information technologies during the last decades of the 20th century and the first decade of the current century have had dramatic changes in many aspects of society. Changes in communication's economics enable fast, easy and cheap mass dissemination of information. This dissemination triggers new and innovative solutions, which already affect our lives, and many other potential changes that will follow. A very well-known and successful example is Facebook, the popular online service for social networking. In approximately six years since its launch Facebook has over 500 million users [Facebook, 2010]. However, currently Facebook is much more than a social network, mainly due to additional possibilities exploited by its user community. Utilizing an open development infrastructure enables interested individual engineers and organizations to develop additional services to be integrated in the system and be available to all its users. Furthermore, for enhancing the social experience, Facebook developed several Software Development Kits (SDKs) that provide a two-way communication between any website and Facebook. Users and organizations are using the Facebook platform in new ways, some that were not originally anticipated by its creators. The wealth of available applications and uses were driven mainly by user needs and ease of implementation. Facebook provides diverse means for content creation including links, stories, blog posts, photo albums and many others. The new technologies, particularly ICT (Information and Communication Technologies), for which Facebook is a concrete example are having an enormous social and economic impact and are the force behind the transition to a post-industrial information society [Masuda, 1980]. The new information society, in which knowledge plays a significant role, raises new ethical issues, ranging from access and intellectual property rights to individual dignity, privacy, and security [Petrovic-Lazarevic and Sohal, 2004]. For that reason many scholars have addressed implications of the Internet and the new information technologies for law and society.

## 2. Generational Differences

Generational research that started to appear in scientific papers over half a century ago was first attributed to Karl Mannheim [1952], who analyzed the impact of generational experience on people. Since then, the generational cohort was developed and is used to define a group of people who were born within the same time period. The group experience similar events that shape its attitude and traits [Jones et al., 2007]. According to Strauss and Howe [1991], who researched similarities and differences between generations over 550 years, one cycle of history spans about 80 years and is divided into four turnings or generational cohorts. The last four generations in the 20th century are:

1. The Silent Generation (also referred to as The Mature Generation, Traditionalists or The Greatest Generation), who were born prior to 1946. This generation, which was influenced by the two World Wars and the Great Depression, is considered loyal, collaborative, shares values and behaviour and is willing to sacrifice personal interests for the common goal [Lancaster and Stillman, 2002; Reesor and Schlabach, 2006].

2. The Baby Boomers (also referred to as the Boom Generation), who were born between 1946–1964. The term was used to define the “boom” in the birth rate in the post WWII era. This generation was affected by events, such as the Vietnam War, the human rights movement, rock and roll, the arrival of television and economic prosperity. This generation is considered to be idealistic, optimistic and highly competitive [Lancaster and Stillman, 2002; Reesor and Schlabach, 2006].

3. Generation X, who were born between 1964–1980, were affected by new media channels, beyond television, including games, video cassette recording (VCR), fax machines and the personal computer. This generation saw the fall of the Berlin Wall and end of the Cold War. People in this generation are considered to be sceptical and independent, relying on their individual abilities rather than institutional help [Lancaster and Stillman, 2002]. People belonging to this generation went to college between 1979–1999 [Coomes and DeBard, 2004].

4. Generation Y (also referred to as Gen Y, The Net Generation, Millennial, Generation ME or The Digital Generation), were born between 1981–2000. People belonging to this generation were influenced by the rapid expansion of technology and media, violence, widespread drug usage and unprecedented immigration growth [Lancaster and Stillman, 2002]. The Millennials are the most technological savvy generational group, feeling confident and natural using a variety of technologies (mobile phones, person digital assistants (PDAs), computers, games, electronic gadgets, etc.). Generation Y people use the Internet extensively for finding solutions to their problems and expect to be in touch constantly with friends and peers using short message servicing (SMS), instant messaging (IM),

chat, and social networks. If consistent with their referent research, they depend on their social network to answer problems. They even tend to prefer Internet networking over telephone-based voice communication [Oblinger, 2003].

### 3. The Digital Economy

We are witnessing a paradigm shift from the old traditional industrial economy to a new economy characterized by information, services and intangible resources. Many scholars have addressed the new forming economy, using names like “borderless economy”, “networked economy”, “knowledge-based economy”, “the information based economy” and “digital economy” [Woodall, 2000; Sharma et al., 2004], to name a few. This “digital economy” has changed business practices, work organizations and institutional structures. In essence, the digital economy is about using information and communication technology (ICT) for coordination, innovation, selection and learning [Gärdin, 2002], creating new and novel business models. The digital economy is expanding the economic potential [Persaud, 2001] by utilizing the new business models and using information and ideas rather than tangible materials. As such, the business focus has moved towards creation, maintenance, distribution and trading of knowledge. An important foundation of the digital economy is the formation of service-oriented business practices, and even large manufacturers are required to augment services and information in their products [Gärdin, 2002]. ICT usage is not limited only to the definition and creation of the new services, but also provides the means for measuring QoS (quality of service). QoS is a broad term that was originally used to measure telecommunication networks’ performance. However, currently, it is generally used to describe the overall user experience when using a product or a service. The QoS measurement and analysis combines two aspects: the product/service attributes; and the customers’ opinions after using it. While for the product or the service, the developing organization has some information (quality, price, time to market, etc.), additional data regarding competition has to be gathered from various sources. User experience, on the other hand, although can be estimated, has to be compiled and gathered, using mainly external sources (representing the users or their actions). This is required for achieving an extended connection between long-term requirements engineering and business-oriented planning [Lehtola, et al., 2009].

The rapid technological development (both hardware and software) has advanced storage technologies as well as the means for data acquisition. The vast amounts of data accumulated by commercial and non-profit organizations, such as supermarkets, credit card companies, telephone companies, service providers and even governments has generated the need to analyze large databases, looking for hidden patterns and relationships. This process of knowledge dis-

covery is the basis of a relatively new set of tools and methodologies for data mining. In their book *Principles of Data Mining* [Hand et al., 2001], the authors state that “Data mining is the analysis of (often large) observational data sets to find unsuspected relationships and to summarize the data in novel ways that are both understandable and useful to the data owner”. For commercial organizations, extracting the information provides additional value in an attempt to improve the customers’ experience. There are many scientific approaches to data mining, however, the important issue relates to the fact that data mining deals with observational data that represents past behaviour. Contrary to experimental data, mining observational data provides a higher degree of accuracy, creating an enhanced, more reliable decision support system. In most cases data mining is performed on data already accumulated by the organization, such as transaction data in a supermarket, telephone call details or credit card usage records [Claus et al., 2002].

#### 4. Common Technologies

The extensively used HTTP (Hypertext Transfer Protocol, which is the foundation of data communication on the web) works in a client server mode. First, the client (the user web browser) sends a request to the server. This request may be either for receiving some information or to execute an application. The server executes the request and sends back the response. At that stage the connection between the client and the server is dropped due to the fact that HTTP maintains no linkage between requests and treats each request independently. However, many web applications have a need to maintain some linkage between current and previous requests, for example, preserving previous preferences or pages visited, etc. To support new business models in the digital economy, and provide a better user experience, several technologies have been implemented. The first and most widely used mechanism is cookies, which, for web applications, provide the means to authenticate the client and maintain its states and preferences. Relating to the digital economy, many online shopping applications maintain the shopping cart, even if the previous visit to the site was weeks or months earlier. For establishing the linkage between requests, web applications often use cookies. A cookie is a piece of information up to 4KB (kilobytes, or 4096 bytes) per Internet domain, stored on the client side, which records information [Liu, et al. 2005]. The cookie is used in future requests for identifying the client, its state and preferences. There is much vulnerability associated with cookie technology that can be used for malicious attacks, such as information leakage, in which sensitive information is transmitted to other parties, session hijacking, which means taking control of a user session after successfully obtaining or generating an authentication session ID, code injection and many more. Nevertheless, the



mechanism is still widely used. However, due to the inherent cookie limitation (4KB per Internet domain), other additional technologies were developed. Adobe Flash by Macromedia, which is used to add interactivity to web pages, uses up to 100KB, without the user's interactions and an unlimited amount after accepting the user's agreement. Microsoft in its Internet Explorer Persistence of user data uses a special file to store up to 64KB per page. The increased storage capacities utilized by the two technologies significantly increase the amount of information stored locally, which in turn amplifies the security risks involved.

In his book *Mass Customization* [Pine, 1993], Joe Pine analyzes the market trends and argues that organizations will have to abandon the old way of doing business, by utilizing mass production where "standardized products, homogeneous markets, and long product life and development cycles were the rule" and adopt to a new world characterized by "variety and customization supplant standardized products". Pine emphasizes that in the new digital economy developing just one product does not meet the users' requirements and is not sufficient anymore. This means that organizations will have to augment their products' offering and provide multiple products that address many requirements represented by many customers. E-commerce, or performing commerce in the digital world addresses some of the issues raised by Pine. It does not provide a mechanism for developing more products; however, it does provide the means for customization, which presents more choices and a higher degree of flexibility for the customers. Jeff Bezos, Amazon's Chief Executive Officer (CEO) is widely quoted as saying: "If I have 3 million customers on the Web, I should have 3 million stores on the Web" [Schafer et al., 2001]. The understanding that customers should be provided with a high level of customization, almost as if it was a totally different store, is one of Amazon's – a leading e-commerce enterprise – success factors. Although Amazon offers million of titles to choose from, the system presents customers with a new buying experience designed to ease the information overload. The system applies mass customization principles to the products' representations rather than to the products themselves [Pine and Gilmore, 1999], by offering many personal search capabilities, including suggestions based on previous preferences. The once innovative technique is currently a common practice and is addressed by all recommender systems [Schafer et al., 2001] that are widely used as an integral part of most e-commerce sites. Recommender systems collect, analyze and use product knowledge accumulated from various sources. Using this knowledge the recommender systems provide consumers with intelligent suggestions and guide them in their search for the best product or service to suit their needs. Many organizations, such as Amazon.com, Netflix.com, Half.com, CDNOW, J.C. Penney, and Procter & Gamble have been using recommender systems, which lead to an increase in web sales and better customer loyalty [Huang et al., 2007].

Most recommendation technologies use various algorithms for analyzing three types of data: products, consumers and previous interactions between the two.

Utilizing ICT for business purposes and developing an e-commerce infrastructure have significant advantages for organizations of all types. The online platform overcomes normal and physical limitations, and provides a global exposure and 24/7 availability. In addition, e-commerce reduces costs associated with production and marketing, lowers inventory costs and improves organizational efficiency [Sharma and Gupta, 2003]. These new benefits provide extensive opportunities for organizations in offering new services and products at a lower price, just by integrating Internet-based systems and business models. The next stage, as predicted by the “square wheel” model [Benson and Parker, 1988] involves redesigning business processes to produce more value and increase competitiveness. As most organizations have adopted the new technologies and have been transformed into digital firms, the pressure for additional new innovations is increasing. This leads to a continuous improvement process that is required for creating a more agile organization, capable of dealing with future market opportunities. After lowering costs, establishing a more efficient organization, providing global presence and continuous (24/7) operations, and forming close relations with customers and business partners, organizations were looking for additional commercial and marketing benefits to be gained from using ICT. Utilizing storage and computational resources for collecting and analyzing large amounts of digital information is a common practice among most organizations. This has been followed by a rise of data mining tools for discovery of hidden information that could not be easily seen. Combining information gathered from various online sources is extremely valuable and provides online commerce organizations with the opportunity to collect relevant marketing information and learn more about customers, their behaviour and preferences. This accumulated knowledge that relates to products, consumers and previous interactions between the two is used by the recommender systems. These systems recommend new products, services or usage patterns, which in turn starts a new cycle of information gathering. Combining consumers’ innovative usage with recommender systems creates a balanced and efficient mechanism of information sharing between consumers and retailers, and vice versa. New ideas regarding products’ capabilities flow from the consumers to the retailers, who in turn feed them back to the consumer community as recommendations. This mechanism enhances products’ visibility, increases sales and profits and when combined with the right ICT platforms (Facebook for example), can be employed at an increasing pace.

## 5. Data Mining on the Web

In her book *The Gift of Fire* [Baase, 2008], the author draws a comparison between fire and computer systems. Like fire, which was given to humans, and enhanced their lives, but also caused some terrible disasters, so computer systems enhanced human lives, but also created undesired and dangerous situations. One of these potentially dangerous situations is the fact that being active on the web, even by just browsing, leaves a digital trail. Individuals often provide personal information required by the system they are connected to. This information may include name and address (shipping address, for example, credit card information for billing and even just names for registrations and when joining various web forums). However, this simple and naive information sometimes provides valuable knowledge. By using common Internet technologies (e.g. cookies), various software pieces integrated into the browsers provide advanced capabilities for collecting this type of information without the user's knowledge or consent.

An important technological advancement that was developed during the last decade is a set of tools, protocols and systems, referred to as Web Services [Alonso et al., 2004] that exchange data autonomously between different web-based systems. One of the aims in developing Web Services was to provide the required capabilities in defining a virtual computing platform in which millions of information systems can share their resources. As far as e-commerce is concerned, Web Services provide the capabilities for supporting complex transactions, in which more than two parties are involved (e.g. consumer, retailer and an external service provider for credit card authentication and clearance). Web Services capabilities, however, are used for a new generation of data mining applications that exchange personal information gathered from the customer's visits at multiple sites.

When placing online orders, the consumer has to provide some personal data (name, shipping address and billing information) in order to finalize the transaction. Some online shops may require additional information sometimes obtained during registration, such as password, date of birth, etc. Most e-commerce software packages use secured protocols for ensuring data privacy and to prevent malicious attacks. However, by using Web Services the same software packages are sharing some data items with third party organizations, such as credit card clearing houses or delivery companies. When considering consumer data privacy, a second, more dangerous, source of data is available. Every activity or interaction on the web leaves clearly detectable traces. By collecting and analyzing these traces the user's behavioural patterns can be easily drawn. For years, Amazon, for example, has provided an enhanced shopping experience by collecting not only sales information, but browsing behaviour as well. A returning customer is

presented with the list of items they browsed in previous visits. This is done by integrating the data stored in the cookie with additional data stored on Amazon's systems. The main concern and threat caused by this type of personalization and integration is the loss of anonymity [Chellappa and Sin, 2005]. The naïve consumer browses the web assuming their anonymity is maintained; however, by using data stored in the cookies and sessions' logs, the web applications easily reveal the user identity [Srivastava et al., 2000]. These new (dangerous) capabilities were rapidly exploited. Originally, the cookies mechanism was used for targeted advertising based on keywords found during browsing. The next stage, of data integration, provides a much better success rate since it augments current browsing with previous behaviour patterns. As such, recommender systems may suggest relevant products that are not directly related only to the current browsing session. The main reason behind the development of such recommender systems is the understanding that these systems provide added value for the retailers. Unfortunately, these benefits, in many cases, are at the expense of sacrificing consumer privacy. More critical examples may involve the selling of private information related to patients' medical conditions. Such examples are not new as stated by the *Washington Post* in an article dating back to 1998, about CVS (The largest pharmacy drugstore chain in the US), sharing prescription records with a direct mail and pharmaceutical company [O'Harrow, 1998]. With the new Web Services technologies, sharing consumer information, including private facts is very easy, and it unfortunately supports the famous saying attributed to Scott McNealy, CEO of Sun Microsystems, who said in 1999: "You have zero privacy anyway. Get over it".

## 6. The Right to Privacy

Most Western cultures and civilizations are built on principles of freedom and individual rights, including the right for security and privacy. Unfortunately recent events undermine the two. On the one hand, the increased terror threats require a higher degree of security that is sometimes achieved at the expense of privacy, as was clearly demonstrated by the new imaging machines used to scan passengers at airports. On the other hand, the rapid technological advancement clashes with "the right to be let alone", as defined by U.S. Supreme Court Justice Louis Brandeis [Warren and Brandeis, 1890]. Although most people will agree that privacy has to be respected, their definition of privacy may vary. This relates not only to scholars and policy makers who are debating the proper privacy definition, but to the whole population, as was clearly demonstrated by WikiLeaks, which is a non-profit organization that publishes mainly private, secret and classified information. The fact that there are various websites that publish all sorts of information, is not new, however, the enormous levels of support WikiLeaks receives from the

public, as well as from news reporters, reputable magazines, organizations and even governments is overwhelming. This support is even more troubling considering the fact that many articles relate to specific identified persons whose privacy and sometimes even personal security was harmed without a second thought. Ignoring online users' privacy is not a new trend. It started with the first electronic mail systems that used to analyze mail content and display targeted advertisements. Later the method was used by various search engines, which scanned search keywords and used some recommender systems for focused advertisements. Marketing efforts, however, did not stop at displaying advertisements, but moved to a more intrusive method of sending unsolicited (junk) mails, trying to convince the users to buy something. This junk mail is often sent as "spam" – a single message that is broadcast to many unknown recipients. In many cases, the mail is anonymous and the sender address does not exist, so no reply is possible. According to a report released in May 2009 by the security vendor Symantec, spam mails account for 90.4% of all emails. Spam emails have become a major concern which has been addressed by many researchers. Currently most email systems include some mechanism for filtering these annoying mails. The information overload demonstrated by many spam messages and advertisements is not limited to the Internet. Targeted marketing uses other technologies as well, for example, cellular networks. Many companies offer LBS (Location Based Services) that are no more than an advertisement sent to the consumer based on their location, as received from the consumer's cellular device [Adams et al., 2003]. This once again represents an intrusion to a person's privacy conflicting with U.S. Supreme Court Justice Louis Brandeis' "right to be let alone" [Brandeis and Warren, 1890].

Although most companies have some privacy policies, it seems that in the hunt for knowledge discovery, basic consumers' rights were disregarded. It is not just the matter of unsolicited mails sent by a small company struggling to get some user attention. Even large corporations are ignoring their users' basic rights. A well-known example is related to Google, the largest search engine on the Internet. In an attempt to improve its offerings and increase its customer base, Google released a worldwide web mapping service. Google even provides an API (Application Programming Interface) that through Web Services makes the maps available for many third party application developers to integrate into their products. When additional similar products became available, and in order to increase the Google service value, Google went on to the next stage and offered Google Street View. This is a new service integrated into Google maps that provides a real street view. When combined with mobile devices, this service is of high value in navigation and getting driving instructions. To establish the new service, Google needed to collect the data by filming streets, ignoring the privacy issues of inno-

cent people that were passing by. Furthermore, the images were uploaded to the web and, thus, not only was privacy harmed, but also it became publicly available worldwide. This led to many articles concerning privacy issues being ignored and the fact that the new service may breach some laws [Bodoni, 2010]. As a result, Google and other companies offering street views, started to blur faces and vehicle license plates [Moncrieff et al., 2009]. However, during 2010, after many additional allegations, Google admitted to 'mistakenly' collecting sensitive private data sent over Wi-Fi (Wireless Fidelity) networks while filming the streets. This, of course, led to a wide range of investigations by many European and state governmental authorities, with several court orders blaming Google for violation of data protection laws. One can only wonder how many additional 'mistaken' collections of sensitive and private data are being performed by other Internet companies. On 15 January 2011, Facebook announced it would allow third-party developers to access the home addresses and phone numbers of its users. This was an expected move, since Facebook CEO Mark Zuckerberg has said that his company's mission is to "make the world more open and connected". However, due to the many concerns and criticism expressed by users and security organizations, Facebook decided to suspend the new feature. The Google Street View and Facebook's attempt to share private data are just some examples of the new trends expressed by large organizations in response to some marketing forces that look for better decision support processes, which unfortunately depend on data collected from users [Sitton, 2006]. Unfortunately, these large organizations, which possess the information, are willing to provide it, ignoring the privacy issues involved. Over 20 years ago, James Moor [1985] defined the "policy vacuum" as the main reason for ethical misconduct. This policy vacuum exists when there is no standard policy to govern a computer-related given situation. He referred to the computer technology uniqueness that allows changing the algorithms and creating new solutions for which no policy exists or has even been considered. Unfortunately, over the years, as technology advances, computer processing power increases while the costs decrease. This leads to new possibilities, such as data mining, data matching and integration, and "click trails" recording [Tavani, 1999]. Combining these new capabilities with the ever growing organizations' need for new knowledge, the policy vacuum is still widening, instead of narrowing, and at an increasing pace.

## 7. Generation Y and Privacy Issues

In spite of the efforts by law makers and regulation agencies regarding privacy issues, Generation Y, which represents one of the major groups to use social networking, has different views regarding information sharing and privacy. Like other generations, these views were developed and shaped by events in their

past. While for previous generations, communication with friends meant meeting face-to-face or talking on the telephone, for the current society, communication has many meanings. IM, email, text and video messages, blogs, online communication boards and social networking provide the urge for communication. As a result, the world has become a smaller village, in which geographic distance is no longer a barrier and the flow of information is instantaneous. However, more troubling is the fact that Generation Y members treat their virtual friends as if they were real ones and disclose a great deal of personal information without paying any attention to the fact that the information, in many cases, is publicly available for whoever is looking for it. This concern was intensified by conclusions of a recent survey conducted by the Pew Research Center's Internet and American Life Project and Elon University's Imagining the Internet Center [Anderson and Rainie, 2010]. According to the survey, the Millennials will continue to share personal information and most of them will make it a lifelong habit. The survey revealed that many Millennials believe that disclosing personal information to online friends holds many social benefits as people open up to others, creating new friendships, joining communities, seeking help and satisfying the need to belong and be accepted. Millennials, who were the first to utilize the social networks, were already exposed to the benefits, which are the main reason behind their continued pattern of usage, including personal data disclosure. Facebook CEO Mark Zuckerberg addressed this issue at the 2009 Crunchies Award and declared that current web users have become more accepting of information sharing and that privacy has become less of a "social norm". When compared to previous generations, for Millennials, privacy has a very different meaning. This meaning was shaped, following a shift in human identity and activities as part of communities. These social changes are further fuelled by the rapid technological developments and, especially, the new enhanced capabilities achieved by the usage of mobile devices. The always connected paradigm is exploited by Millennials not only to improve information sharing, but also to provide it instantly while disclosure events are happening. The new advanced capabilities provided by the social networks can sometimes be exploited and misused. For example, re-establishing connections with old friends and virtually meeting new ones, which is a cornerstone in any social network may be responsible for creating jealousy and suspicion in romantic relationships [Muise et al., 2009] and has been blamed for an increase in the number of marital breakdowns [The Telegraph, 2009].

## 8. The Real Problem

Social networks and the digital economy are two of the many modern trends that coexist. However, the combination of social networks, or the public information stored in them, and the digital economy holds a real threat to privacy. One of

the main forces behind the digital economy is using ICT for coordination, innovation, selection and learning [Gärdin, 2002]. ICT provide essential knowledge for creating new and novel business models. Organizations use and develop ICT-based tools and methodologies to gather accurate and reliable user information. This information sheds light on the users' perspectives and requirements and provides the necessary knowledge for designing new, more effective and competitive products and services. Many technologies were developed to support the process of information retrieval, and all involve mining mechanisms and a wealth of theories for calculating and estimating the information value and accuracy. However, considering the richness and the easy accessibility of the information available as part of the social networks, many organizations' data mining efforts were directed towards social networks. The Internet, in general, and social networks, in particular, play an increased role in research and investigation related to due diligence, background, employment and skip tracing investigations as well as reputation research and even surveillance for legal and insurance matters [Thompson, 2007]. Numerous studies analyze the various types of information found on social networks [Gross and Acquisti, 2005; Muise et al., 2009] and how this information can be exploited. More interesting, however, are various correlations performed on the information, for example, mining comments entered by teens for collecting information on their other family members. This information can be just background data, employment-related, and even as a basis for insurance claims denial. In a paper by Latanya Sweeney [2000], gender, birth date and ZIP code are sufficient to identify 87% of the U.S population. Mining these three items and correlating them with other data from different sources can be used for sophisticated processes of decision making. It is not clear how much information is obtained from social networks data mining, or by whom. However, in a *Wall Street Journal* article by Laura Saunders [2009], the author describes cases in which state revenue agents and authorities have been mining information posted on social network websites. In a different *USA Today* article, Kevin Johnson [2010] states that "law enforcement agencies are digging deep into the social media accounts of applicants, requesting that candidates sign waivers, allowing investigators access to their Facebook, MySpace, YouTube, Twitter and other personal spaces". Another example is an article by John Oates [2008] about 13 Virgin Atlantic employees who were fired for their comments on Facebook. These types of practices are so widely used by industries that in August 2010 a draft law that bans Facebook research for hiring decisions was approved in Germany. Employers will be allowed to look for information regarding the applicant, using various search engines and social networks, but they are not allowed to look at their Facebook profile. This German law represents a new way of thinking. It not only examines traditional law in the new environment, but tries to define new laws needed to deal with the situations and problems that technology has cre-



ated. Using technological tools, new sophisticated cyber-crimes, in which hackers target social networks for planning malicious attacks and stealing user identities, have become very common. The new law does not address these criminal acts in a new setting; it tries to address a common and ordinary practice of using the widely available public data for better and legitimate decision making processes. However, since social networking sites have become a well-known source of information, many lawyers, private investigators, law enforcement agencies, employers and organizations are using these new capabilities. The new law is the first step in the right direction; however, it addresses only potential employers. The notion that every individual is responsible for protecting their personal information may have been valid for prior generations. Millennials, who record their lives, almost in real time, falsely believe that the information is shared only by “real” friends, and have to be better protected, especially, since every piece of information, even if deleted, will last for a very long time.

## 9. A Concluding Remark

Technology is moving forward at an increasing pace and it will continue to advance in the foreseeable future; Millennials will continue to expose their lives, ignoring potential negative implications and undermining the “old” privacy norms. These two combined trends lead to large and fast growing volumes of public information. Utilizing already available data mining tools provides a wealth of benefits for an increasing number of organizations and commercial companies. The new knowledge obtained will create new demands for additional, more sophisticated tools for mining and correlating information from various sources. What is missing and increasingly required are the proper definitions of limits and boundaries. Unfortunately, Millennials do not pay any attention and continue posting growing pieces of their lives, actions that cannot be undone. Usually, people know it is forbidden to use a credit card even if it was found on the street. However, using other and sometimes much more sensitive personal information obtained on the web is considered to be legitimate. Laws that regulate conflicting interests should play a more active role, balancing “the right to be left alone” and “the right to know”. It is time for some new laws to address the policy vacuum that continues to widen quickly, or else, current innocent social networks’ status updates may become future evidence.

## References

Adams P., Ashwell G., and Baxter, R. (2003). Location-based services – an overview of the standards, *BT Technology Journal*, 21(1), 34-43

Alonso G., Casati F., Kuno H., and Machiraju, V. (2004). *Web Services: Concepts, Architectures, and Applications*. Springer-Verlag, Berlin/Heidelberg, 2004

Anderson J. and Rainine, L. (2010). Millennials will make online sharing in networks a lifelong habit. Online at <http://pewinternet.org/Reports/2010/Future-of-Millennials/Overview/Overview-of-responses.aspx?r=1>/accessed December 20 2010

Baase S. (2008). *A gift of fire – social, legal and ethical issues for computers and the Internet*, Prentice Hall.

Benson R J., and Parker, M. M. (1988). *Information economics: Linking business performance to Information Technology*, Prentice Hall.

Bodoni S. (2010). Google street view may breach EU law, officials say. Online at <http://www.bloomberg.com/apps/news?pid=20601085&sid=a2Tbh.fOrFB0/> accessed December 23 2010.

Chellappa R.K., and Sin, R.G. (2005) Personalization versus privacy: An empirical examination of the online consumer's dilemma, *Information Technology and Management*, 6, 181-202.

Claus B., Günther O., and Teltzrow, M. (2002) Privacy Conflicts in CRM Services for Online Shops: A Case Study. *Proc. IEEE Workshop on Privacy, Security, and Data Mining*, Volume 14 of the *Conferences in Research and Practice in Information Technology*, 2002.

Cnet Report (2009). Report: Spam now 90 percent of all e-mail. Online at [http://news.cnet.com/8301-1009\\_3-10249172-83.html/](http://news.cnet.com/8301-1009_3-10249172-83.html/) accessed December 10 2010

Coomes M.D., and DeBard, R. (eds.) (2004) *Serving the Millennial generation*, Jossey Bass.

Facebook Statistics. (2010). People on Facebook. Online at <http://www.Facebook.com/press/info.php?statistics/> accessed December 21 2010

Gärdin O. (2002). The new economy new challenges for the statistical system. *The International Association for Official Statisticians Conference*, London 2002.

Gross R., and Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society (2005)*, pp. 71-80.

Hand D. J., Mannila H., and Smyth, P. (2001). *Principles of data mining*, MIT Press. pp. 1.

Huang Z., Zeng D., and Chen, H. (2007). A comparative study of recommendation algorithms in e-commerce applications, *IEEE Intelligent Systems*. 22(5), pp. 68-78

Johnson K. (2010). Police recruits screened for digital dirt on Facebook, etc. *USA Today*. Online at [http://www.usatoday.com/tech/news/2010-11-12-1AFace-bookcops12\\_ST\\_N.htm/](http://www.usatoday.com/tech/news/2010-11-12-1AFace-bookcops12_ST_N.htm/) accessed January 15 2011

Jones V., J. Jo, and Ph, M. (2007). Future schools and how technology can be used to support Millennial and Generation-Z students. *ICUT 2007 (Proceedings B)*, 1<sup>st</sup> International Conference of Ubiquitous Information Technology, Dubai, February 12-14, 2007, pp. 886-891.

Kehal H., and Varinder, P.S. (2005) *Digital economy - Impacts, influences and challenges*, Idea Group Publishing,

Lancaster L.C. and Stillman, D. (2002) *When generations collide who they are. Why they cash. How to solve the generational puzzle at work*, Harper Business.

Lehtola L., Kauppinen M., Vahaniitty J., and Komssi, M. (2009). Linking business and requirements engineering: Is solution planning a missing activity in software product companies? *Requirements Engineering*, 14(2), 113-128.

Liu A. X., Kovacs J. M., Huang C., and Gouda, M. G. (2005). A secure cookie protocol. *Proceedings of the 14th IEEE International Conference on Computer Communications and Networks* (pp. 333-338). San Diego, CA.

Mannheim K. (1952) *Essays on the sociology of knowledge*, Routledge & Kegan Paul Ltd.

Masuda Y. (1980). Computopia: Rebirth of theological synergism. In Masuda, Y. (Ed.), *The information society as post-industrial society*. Tokyo: Institute for the Information Society and 1981 by World Future Society.

Moncrieff S., Venkatesh S., and West G. A.W. (2009). Dynamic privacy in public surveillance, *Computer*, 42(9), 22-28.

Moor J. H. (1985) What is computer ethics? (ed. T. W. Bynum), *Computers & Ethics*, 266-275

Muise A., Christofides E., and Desmarais, S. (2009). More information than you ever wanted: Does Facebook bring out the green-eyed monster of jealousy? *CyberPsychology & Behavior*, 12(4), 441-444.

Oates J. (2008). Virgin sacks the Facebook. *The Register*, 3 November, 2008. Online at [http://www.theregister.co.uk/2008/11/03/virgin\\_sackings\\_ba\\_rudeness/](http://www.theregister.co.uk/2008/11/03/virgin_sackings_ba_rudeness/) accessed January 20 2011

Oblinger D. G. (2003) Boomers, Gen-Xers & Millennials: Understanding the new students, *EduCAUSE Review*, 38(4), 37-47.

O'Harrow R. (1998). Prescription fear, privacy sales, *The Washington Post*, February 15, 1998, A1.

Persaud A. (2001). The knowledge gap, *Foreign Affairs*, 80(2), 107-117.

Petrovic-Lazarevic S., and Sohal, A. S. (2004). Nature of e-business ethical dilemmas, *Information Management & Computer Security*, 12, 2, 167-177.

Pine II B.J. (1993). *Mass customization*, Harvard Business School Press. pp. 34

Pine II B.J., and Gilmore, J.H. 1999. *The experience economy*, Harvard Business School Press.

Reesor L., and Schlabach, K. (2006). Managing multi-generations: Strategies for crossing the generational divide in the workplace, *NASPA Leadership Exchange*, 4(3), 16-19.

Saunders L. (2009). Is 'friending' in your future? Better pay your taxes first. *The Wall Street Journal*. 27 August, 2009. Online at <http://online.wsj.com/article/SB125132627009861985.html>/ accessed January 5 2011

Schafer J.B., Konstan J.A., and Riedl, J. (2001). E-commerce recommendation applications, *Data Mining and Knowledge Discovery*, 5, 115-153.

Sharma S. K., Wickramansinghe N., and Gupta, J.N.D. (2004). What should SMEs do to succeed in today's knowledge-based economy? In N. Al-Qirim (Ed.), *Idea Group Publishing*.

Sharma S. K. and Gupta, J.N.D. (2003). Creating business value through E-commerce. In N. Shin (Ed.), *Creating business value with Information Technology: Challenges and solutions*, Idea Group Publishing.

Sitton J.V. (2006) When the right to know and the right to privacy collide, *Information Management Journal*, 40(5), 76-80.

Spernger P. (1999). Sun on privacy: 'Get over it', *Wired News*, 26 January 1999. Online at <http://www.wired.com/news/politics/0,1283,17538,00.html>/ accessed February 10 2011

Srivastava J., Cooley R., Deshpande M., and Tan, P.-N. (2000). Web usage mining: Discovery and applications of usage patterns from web data, *ACM SIGKDD Explorations* 1(2), 12-23

Strauss W., and Howe, N. (1991) *Generations: The history of America's future, 1584 to 2069*, William Morrow.

Sweeney L. (2000), Uniqueness of simple demographics in the US population, LIDAP-WP4. Carnegie Mellon University, Laboratory for International Data Privacy.

Tavani H.T. (1999). KDD, data mining, and the challenge for normative privacy, *Ethics and Information Technology* 1(4), 265-273.

The Telegraph (2009). Facebook fuelling divorce, research claims. Online at <http://www.telegraph.co.uk/technology/Facebook/6857918/Facebook-fuelling-divorce-research-claims.html/> January 22 2011

Thompson T. (2007). The armchair investigator: Social media and teens. The Pew Internet & American Life Project report. Online at <http://pibuzz.com/2007/12/24/the-armchair-investigator-social-media-and-teens/> accessed January 20 2011

Warren S., and Brandeis, L. (1890). The right to privacy, *Harvard Law. Review*, 4(5), 193-220

Woodall P. (2000). Survey: The new economy: Knowledge is power. *The Economist*, 356(8189), 27-32.

# Technology beats the law?

---

---

Georgios Yannopoulos

---

---

## 1. Empirical Input

### *Example I*

Under article 1176 par. 1. sec. 1 and article 1244 par. 1 of the Greek Civil Code, shares may be charged with a pledge and/or usufruct; the same rules apply for dematerialised securities traded in the Greek Stock Exchange as specified under articles 48 par. 2 (*Registration of Pledge on Securities*) and 49 par. 2 (*Registration of Usufruct on Securities*) of the Regulation on the Operation of Dematerialised Securities System (DSS, Decision 3/304/10-6-2004 of the Board of the Greek Capital Markets Committee, Official Gazette B' 901/16-6-2004, as in force). However, until recently, if someone tried to charge securities, already under usufruct (considered as a first charge), with a pledge (considered as a second charge), the system was not able to register the second charge, simply because there was no field provided for; DSS had not been designed to accommodate simultaneously two of the most common charges of the Greek Civil Code, functioning in (materialised) legal practice for over sixty years.

### *Example II*

In July 2010 academics and the judiciary in Greece were upset; the judiciary even threatened to cease performing their duties. The Greek state had organised a nation-wide census in order to register electronically in a database and identify all personnel (public servants) paid under the state payroll (as per Law 3845/2010 and Ministerial Decision 2/37345/0004/4-6-2010). The relevant field in the database had been designated “public servants”. However, according to Article 16 par. 6 of the Greek Constitution “Professors of universities shall be public *functionaries*”; moreover art. 88 par. 1 designates judges as “*functionaries*” not “servants”. The protesters (judges and professors) have claimed that the design of the user interface of the database had ignored critical legal parameters and, as a consequence, it had diminished their status, which is defined by law.

### ***Example III***

Under art. 1 par. 1 of Greek law 5638/1932 two or more persons may open a joint account at a bank operating in Greece; the law does not distinguish between natural or legal persons. However, if someone tries to open, at a bank, such joint account for two legal persons this is not possible; the computer system, of several major banks operating in Greece, does not provide adequate “space” for the legal representatives of two legal persons.

## **2. What System Analysis is required**

According to the basics of computer science, a system analysis is a traditional *sine qua non condition* before any attempt to computerise a manual procedure. The effort to analyse a certain domain, normally takes the form of a comprehensive description, writing down and sketching parts of the system’s functioning and basic characteristics as a precondition to the analysis (LoPucki, 1997). In the same vein, if we want to create legal applications i.e. computer applications that transform “manual” legal procedures into automated ones, such analysis must pave the way for any attempt to write down the source code of any software. The concept of “systems analysis” described in this paper is an empirical cumbersome procedure, since the legal phenomenon must be seen and examined under the eyes of a technically oriented analyst, who will gather the necessary knowledge. The analyst normally creates the input material to be processed at the next stage by the computer programmer, who will then write the lines of the source code i.e. the set instructions (the software) to instruct the machine. It is evident that such an analysis has also been followed in all of the above examples: all three applications seem to work properly - in terms of computer programming - but they produce erroneous results, not acceptable by lawyers, or at least upsetting them. The empirical investigation reveals that in the three examples, not only a legal analysis is missing, but critical aspects of law are simply ignored, just because there is not enough space on the monitor screen. Computer programmers, in seeking technical perfection had not realised the importance of the legal rules. As a consequence, the end product does not obey the law and hence, the technical qualifications of the systems’ analyst fall short of their endeavours: “*the system is doing things and producing results that participants in the system did not intend or anticipate*” (LoPucki, 1997).

The contradiction is being exaggerated to the eyes of an average practitioner, because, in his/her view, even law undergraduates would be able to foresee and point out the necessary fields in designing the databases and the user interface of the applications in the three examples:

- i) Following the doctrine of liens and charges of the Greek Civil Code, two or more fields should be added for *usufruct* and *pledge* or any other charge over securities,
- ii) Following the distinction of the Greek Constitution, a specific field should be added for “*functionaries*”, apart from the general description for “*public servants*” and
- iii) Following the Greek Law for joint accounts, additional fields and space should be provided for the *representatives* of two or more legal persons.

For a person having formal legal background, these should be the first parameters to examine, before attempting any analysis and subsequent programming.

To make things worse, apart from the above examples, in numerous cases users are forced, under the time pressure of everyday computerised transactions, to consent to such distorted and erroneous application of law and even to accept *contra legem* consequences. It is a common belief that if the computerised system and/or the software dictates so, no other alternative may be followed: “...*Sorry, you cannot have a pledge over shares already charged with usufruct...*”. A stage has been reached at which computer dictators (a.k.a. programmers) supersede established legal doctrines, and impose their own rules. Their effort is being led by the assumption that the features of the technology in question appear intuitively coherent and valid because they are supported by a paradigm of “technological determinism” (Pantaloni, 1994). The result coincides with Lessig’s words that programmers (coders) “...constrain some behaviour by making other behaviour possible or impossible. The code embeds certain values or makes certain values impossible...” (Lessig, 2006). The examples already exposed amount to an understated proof that technology (the code) is a regulatory modality affecting human behaviour. Under that regime, software regulates online behaviour and programmers act like deities, defining the rules of nature online, altering and shaping things that might seem unalterable, maybe even natural” (Ohm, 2009). Such application of scientific methods and analyses leads to a distorted interpretation of the legal phenomenon, which contradicts existing laws and procedures. Systems analysts and computer programmers make inferences on the basis of generalisations about the law and their compartmentalised research obstructs the development of a complete picture of how computerised applications may change the nature and functions of the process of law in a society (Katsh, 1984).

In this erroneous model, the social, political or cultural institutions, are underestimated; only the technology counts. Under the analysis firstly introduced by Marshall McLuhan, it would be acceptable for a new technology that comes into a social milieu to permeate that milieu until every institution is saturated (quoted



by Katsh, 1984, footnote 4 and Pantaloni, 1994, footnotes 13, 14). However, would it be acceptable for an institution, such as law, to be shaped and controlled by the medium? Are we obliged to conduct a proper analysis, leading to (legally) acceptable results? In that case, what would then be the determining factor, within the dynamics of the legal system?

The answer is straightforward: when designing and implementing legal applications, the defining factor should be the law and the associated legal system. Jurisprudence must be the guiding force; not computer science. It is beyond doubt that information technology presents advantages and benefits for lawyers. However, while in other disciplines it would be unacceptable to consult an outsider, in the case of law the *quasi*-“dictatorship” of computer programmers is nearly instituted. Computerised applications in law, designed to produce legal implications often ignore fundamental aspects of the legal process and treat law as if it were a guinea-pig without taking into consideration the current state of the law.

The proposed solution is that system analysis must be adjusted to the legal framework and any IT application having legal effects must, in the first place, abide by the substantive, procedural and methodological rules of the particular legal system. The first intuitive move of the analyst would be to consult an expert lawyer i.e. a lawyer with deep knowledge of the substantive and procedural rules of law in a particular area. Under that condition, analysts should possess or try to acquire basic legal knowledge, if not full scale formal legal education. The degree of the knowledge required depends on the difficulty of the task under consideration. To overrule the dictatorship of system analysts and computer programmers, we need computer software that will respect recognised legal procedures and will be based on sound knowledge of legal functions. Such software should be able to create a legal paradigm and should be able to guide and convince even laymen in their everyday practices. The end result, where systems analysis builds upon traditional methods of analysing the law, should lead to technology serving the law not *vice versa*.

### 3. Why? - “The rule of law”

As early as 1977 the “rule of law” has been proposed (Bing & Harvold, 1977) as the basis for the improvement of any legal information system. The “rule of law” is not only the widely accepted cornerstone of modern jurisprudence but also sets the quality standards for the treatment of legal information (Wahlgren, 1999). Two fundamental principles have been postulated (Dworkin, 1986) as the basis inherent to this concept: the *principle of legality* and the *principle of equality* before the law. The first principle reflects the demand for *predictability*, i.e. the necessity within a legal system to predict in advance certain results to respective actions.

This is directly connected to the general principle of “*knowing the law*” depicted by the Latin motto *ignorantia juris non excusat* and in that sense (legal) information must be updated and validated from authoritative sources. The second principle entails that cases, similar from the legal point of view should be decided in the same manner. Official legal decision-making from courts or other authorities should lead to equal treatment of equal cases. This is not merely a purely theoretical view, but a direct expression of the above “rule of law” doctrine: As long as citizens have the right and obligation to “know the law” they also anticipate that computerised applications, having legal implications, comply with the law (Wahlgren, 1999). Furthermore, under that principle, it would be unacceptable to face different “legal” behaviour when a citizen uses a computerised system that a manual one, as it has happened in the three examples under scrutiny

Any legal informational system that does not meet these requirements endangers to lose its authority. Lawyers, in performing their functions in their *law-consulting* or *law-awarding* roles (e.g. judges) are not free to go beyond what is stated explicitly in the law. Under that rule, computerised applications in law must demonstrate an internal consistency with the legal system that they support (Yannopoulos, 1998) and analysts, playing the role of lawyers, are not allowed to supersede the law and go beyond established legal doctrine. Infringing this rule produces technically correct but legally erroneous results and, apart from the legal consequences, results to lawyers and laymen mistrusting modern technology. Apart from the three initial examples, several sound practical computerised applications in the core area of the legal environment have fallen short of the specifications envisaged by their designers and people are simply not using them.

It follows that the theoretical description and the analysis of any IT application in law must be guided by and obey the law, not the technology. In that sense, such computer applications should be carefully tested by persons having legal training, able to verify that the end-results show sound legal consistency with the surrounding legal order.

#### **4. Which legal content to acquire**

The task of finding *what* to include in a legal application has already been emphasised (Yannopoulos, 1998) by our positivist tradition, which has determined a system of clearly defined rules, with a known hierarchy amongst them. This set of objective and identifiable rules is known to legal practitioners well in advance, varying from the scope of macro-level of general norms and principles to the lower micro-level of the particular article or paragraph that regulates a real situation. This jurisprudential notion is being labelled as the *doctrine of valid legal sources* (Wahlgren, 1999). As explained, to produce a useful legal analysis, the analyst

should define the content of a law-related system, having as a guideline the hierarchy of legal sources prescribed by the legal order and, then must empirically test whether the system is achieving to yield practical legal results. The analyst must also include some elements from the surrounding environment and should be cautious because some of the recommended changes may lead to disruption of the basic functions of the system.

Average practitioners are skilful enough to adopt a number of basic standards and to identify the rules that are valid and should be applied at a certain point in time; these rules should be the starting point of research for the lawyer-analyst of computerised legal applications. By order of priority, the lawyer-analyst will:

First, look into the sources of substantive law: the constitution, international treaties, statutes, decrees etc. or case law i.e. various types of court judgements related to the field of law under computerisation.

Secondly, will take into consideration procedural law and methodological rules, especially those procedural rules disqualifying vast amounts of information.

Thirdly, if needed, will identify other sources such as precedents, parliamentary preparatory works, jurisprudence, legal writings etc.

That strategy takes into consideration the traditional approach to law, as a conceptual system, in order to identify rules, which would drive or prevent a lawyer from taking particular matters into account (*supra*: pledge and usufruct, two legal persons in joint accounts) or providing certain kinds of criteria (*supra*: academics are not public servants). Because lawyers, as decision makers, are not free to decide, but their opinion should be guided by law. A clever strategist would place *law-cognoscenti* in such a position who will be skilful enough to choose the complete legal content required, over the existing alternatives. In the words of LoPucki "...legal scholars are the persons in our society best situated to analyze these systems and document them" (LoPucki, 1997).

## 5. Legal Informatics and Future IT Applications in Law

Starting from the empirical input of the three flawed examples, the main objective for this paper has been to revive the jurisprudential debate about how IT Applications in Law should be treated. It has been submitted (Susskind, 1996) that legal practice transformation, due to technology, may not simply be a matter of change of business strategy or personal attitudes, but an immense enterprise involving institutional changes in the whole legal system i.e. *a shift in paradigm*. Before, the vast institutional changes are reached, I would call for a "*return to basics*" strategy: IT applications in law must be guided by and obey the law, not the technology.

Under that strategy, the next objective would be to issue a word of advice about some of the most annoying fallacies one can encounter when dealing with information technology applications in the legal domain. Following the findings of this paper two main suggestions can be put forward:

1. Any IT application, having legal consequences, must in the first place, abide by the substantive, procedural and methodological rules of the particular legal system.
2. Following that suggestion, system analysis must be conducted by persons holding a minimum of legal skills.

Prediction has been a hard task for Pythia in the Oracle of Delphi. It is clear that, currently, there is a need to focus on accurately designed practical applications, which will facilitate the full introduction of modern IT techniques into the legal field (Yannopoulos, 1998) and can prepare the path for the envisaged institutional changes. For the future, I had speculated that computer programmers should not take the responsibility of legislators and that each discipline should not be enslaved to the other (Yannopoulos, 2002). It is in our hands the undertaking to produce law graduates equipped with computer skills and to enforce Legal Informatics as a discipline charged to set the boundaries and the subject matter belonging to the intersection between the two rivals, Law and IT. A comprehensive discipline should be able to impose, theoretically and practically, the necessary weight to the legal analysis preceding any design, analysis and programming of IT applications in law. If we follow a different path we run the risk of technology "beating" the law.

## References

- Bing J. & Harvold T. (1977), *Legal Decisions and Information Systems*, Universitetsforlaget Oslo.
- Dworkin R. (1986), *Law's Empire*, London.
- Katch E. (1984), *Communications Revolutions and Legal Revolutions: The New Media and the Future of Law*, Nova Law Journal, Spring, 1984, p. 631.
- Lessig L. (2006), *Code: and other laws of cyberspace, Version 2.0*, Basic Books, New York (available online under Creative Commons).
- LoPucki L. (1997), *The Systems Approach to Law*, Cornell Law Review, March, p. 479.
- Ohm P. (2009), *Computer Programming and the Law: A New Research Agenda*, Villanova Law Review, p. 117.

Pantaloni N. A. M. (1994), *Databases, Legal Epistemology, and The Legal Order*, Law Library Journal, Fall, p. 679.

Susskind R. (1996), *The Future of Law*, Clarendon press, Oxford.

Wahlgren P. (1999), *The Quest for Law, Law Libraries and Legal Information Management of the Future*, Jure AB, Stockholm.

Yannopoulos G. N. (1998), *Modelling the Legal Decision Process for IT Applications in Law*, Kluwer Law International, The Hague.

Yannopoulos G. N. (2002), *Information Flows in the Internet, Technology & Legal Regulation* (in Greek), Nomiki Vivliothiki, Athens.



## **YOUNG SCHOLARS' FORUM**





# The legal framework of personal data e-processing in the digital environment in Greece

---

---

Konstantina Arkouli

---

---

## 1. Introduction

The digital networks are a significant human achievement and play a major role in our lives. Especially regarding the internet, we should point out that it is thought of as the threshold of a new era in the field of digital networks, on the grounds that its outbreak reversed the traditional communication framework.

The internet as well as the telecommunication networks have the following special characteristics: a. the contribution of subscribers' or users' personal data such as name, surname, telephone number, e-mail address etc to the network service provider, is mostly a precondition for entry to them<sup>1</sup>, and b. the processing of specific personal data by the network service provider is inevitable with reference to the purposes of the conveyance of a communication, the subscriber billing and the interconnection payments. This fact in combination with the potentialities that are placed at human's disposal by the modern technological means makes it easy for administrators of digital networks or third parties, who are instigated by base motives (curiosity, speculation etc), to process illegally the aforementioned personal data<sup>2</sup>.

The numerous menaces of infringement upon the private sphere of users or subscribers of digital networks (for instance phishing, pharming, tapping, intervention or surveillance of communications, hacking, packet-sniffing, spamming, formation of files with "digital profiles" of users or subscribers of electronic communications services etc), which arise from the technological evolution and the rapid development of digital networks, show the dire necessity of outlining clear and articulate rules for the protection of privacy in the digital environment. In this

- 
1. See K. Christodoulou (2006), Protection of personality and contractual freedom in public available networks (*in Greek*), pp. 55-56 · K. Christodoulou (2008), Epitome of Electronic Civil Law (*in Greek*), p. 16.
  2. See Ap. Georgiades, Private law on the threshold of 21<sup>st</sup> century (*in Greek*), Nomiko Vima 2001, 575 · G. Kaminis, Privacy in telecommunications: Constitutional protection and its implementation by the penal legislator and the courts (*in Greek*), Nomiko Vima 1995, 508 · G. Georgiades, The Law No. 3471/2006 about the protection of privacy in electronic communications (*in Greek*), Chronika Idiotikou Dikaiou 2007, 17.

paper, we will present the legal framework of the personal data processing in the field of electronic communications according to the Law No. 3471/2006, which brings into force the dictates of the e-privacy Directive (Directive 2002/58/EC) in the Greek law and order. Especially, we will focus on the principles of personal data e-processing and the rules about the confidentiality of the communications in the digital networks and about unsolicited electronic communications, which are provided in the aforementioned Law.

## 2. Personal data and their categories in electronic communications

Personal data is any piece of personal information – even insignificant – which concerns an identified or identifiable person (e.g. name, surname, occupation, age, religion, political convictions, physical and moral well-being, private life, marital status etc). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity<sup>3</sup>. If a piece of information is not related to an identified or identifiable person, it will not be called personal data<sup>4</sup>. The aforementioned definition of the term “personal data” is extremely broad<sup>5</sup> and is adopted by both the Directive 95/46/EC<sup>6</sup> and the Greek Law No. 2472/1997<sup>7</sup>, which implements the dictates of the above Directive in the Greek legislation.

Concerning the personal data of users or subscribers of electronic communications, these are divided in the following categories, according to the Law No. 3471/2006:

a. “Data in relation to the content of a communication”<sup>8</sup> are the information, which are exchanged or conveyed between a finite number of parties by means of a publicly

---

3. See article 2 (c) of the Law No. 2472/1997 and article 2 (a) of the Directive 95/46/EC.

4. See E. Alexandropoulou-Egyptiadou (2007), *Personal Data (in Greek)*, pp. 33-34.

5. See L. Mitrou (1998), *Technology and personal data protection (in Greek)*, in: *Proceedings of the 7<sup>th</sup> Panhellenic Conference of Commercial Law – Topic: The adjustment of the modern technology in Commercial Law*, p. 195.

6. See Article 2 (a).

7. See Article 2 (a).

8. See G. Georgiades, *The Law No. 3471/2006 about the protection of privacy in electronic communications (in Greek)*, *Chronika Idiotikou Dikaiou* 2007, 22 · Gr. Tsolias, *The telecommunication data in the light of privacy: Problems in view of the implementation of the Directive 2002/58/EC (in Greek)*, *Dikaio Meson Enimerosis & Epikoinonias* 2004, 360 · K. Christodoulou (2008), *Epitome of Electronic Civil Law (in Greek)*, p. 17.

available electronic communications service with the purpose of the achievement of a communication, such as the content of a telephone conversation, a text message (fax, sms, e-mail etc) or a message with multimedia content (mms).

b. “*External data of a communication*” are the information that specify the circumstances, which individualize a communication<sup>9</sup>, such as name, surname and telephone number or e-mail address of the parties, duration of a call, static IP address<sup>10</sup> etc. The “*external data of a communication*” are further categorized as follows:

1. ‘*Traffic data*’<sup>11</sup> means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. Traffic data are particularly telephone number, address, location data, date, exact start time, exact end time and duration of a communication, information related to the protocol and the routing of a communication and billing data.
2. ‘*Location data*’<sup>12</sup> means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. They may refer to the latitude, longitude and altitude of the user’s terminal equipment, to the direction of the travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded<sup>13</sup>.

---

9. See Gr. Tsolias, The telecommunication data in the light of privacy: Problems in view of the implementation of the Directive 2002/58/EC (*in Greek*), Dikaio Meson Enimerosis & Epikoinonias 2004, 360 · Gr. Tsolias, To a modern legal framework for the protection of privacy in telecommunications (Presentation and annotation of the provisions of the Presidential Decree No. 47/2005), Poiniki Dikaosini 7/2005, 794 · G. Georgiades, The Law No. 3471/2006 about the protection of privacy in electronic communications (*in Greek*), Chronika Idiotikou Dikaiou 2007, 22 · K. Christodoulou (2008), Epitome of Electronic Civil Law (*in Greek*), pp. 16-17.

10. A static IP Address is personal data, because it remains unchanged each time the subscriber connects to the internet and is unique world-wide. On the contrary, a dynamic IP address changes each time the subscriber connects to the internet or during the connection. So, it is not personal data, unless the administrator of the website is able to identify the user or subscriber by using the means at his disposal. See relatively I. Igglezakis, The protection of personal data in the Internet – Regulations of national and community Law (*in Greek*), Episkopisi Emporikou Dikaiou 2002, 684 · A. Fragouli, Are IP addresses personal data and which are the consequences? Dikaio Meson Enimerosis & Epikoinonias 2/2008, 198 · T. E. Synodinou (2008), Intellectual Property and new technologies – The relation between user – creator, p. 286.

11. See article 2 (3) of the Law No. 3471/2006 and article 2 (b) of the Directive 2002/58/EC.

12. See article 2 (4) of the Law No. 3471/2006 and article 2 (c) of the Directive 2002/58/EC.

13. See the 14<sup>th</sup> recital of the preamble of the Directive 2002/58/EC.

### 3. The scope of the Law No. 3471/2006

The first chapter (articles 1-17) of the Law No. 3471/2006 contains the provisions, which bring into force the dictates of the e-privacy Directive in the Greek law and order. The aforementioned articles apply to the processing of personal data and the protection of privacy in connection with the provision of publicly available electronic communications services in public communications networks. On the contrary, the general provisions of the Law No. 2472/1997 are applicable to the personal data processing that is carried out in connection with services provided by means of an intercommunication system of a company, since the case in question is beyond the scope of the Law No. 3471/2006.<sup>14</sup> So, if a network operates not only as a public communications network but also as an intercommunication system, the public communications network is governed by the provisions of the Law No. 3471/2006 and the intercommunication system is governed by the provisions of the Law No. 2472/1997.<sup>15</sup>

Regarding the subjective scope of the Law No. 3471/2006, it concerns not only individuals, but also legal entities. Though the protection of the “*private sphere*” of legal entities finds its basis in the article 9A of the Greek Constitution<sup>16</sup>, the Law No. 3471/2006 is the one and only Greek Law about personal data protection, which provides directly for protection of the legitimate interests of subscribers who are legal entities<sup>17</sup>. This legal regulation complies with the e-privacy Directive<sup>18</sup> and answers practical purposes, which are summarized to the predicament of the providers of electronic communications services to process in a different way the personal data in view of whether they concern individuals or legal entities.<sup>19</sup>

---

14. See article 3 § 1 of the Law No. 3471/2006.

15. Compare to V. Tountopoulos, Protection of personal data in the field of telecommunications – The implementation of the Directive 97/66 in the Greek legislation (*in Greek*), Dikaio Epixeiriseon & Etaireion 5/2000, 477.

16. See K. Christodoulou (2006), Protection of personality and contractual freedom in public available networks (*in Greek*), p. 102.

The article 9A of the Greek Constitution provides that “Everyone has the right of protection from the collection, processing and use, especially by electronic means, of his personal data, as specified by the Law.”

17. See E. Papakonstantinou, Comment for the Law No. 3471/2006 (*in Greek*), Efimerida Dioikitikou Dikaio 4/2006, 444.

18. See article 1 § 2 of the Directive 2002/58/EC.

19. See I. Igglezakis (2006), Introduction to the law of informatics (*in Greek*), pp. 197-198 · I. Igglezakis (2008), Law of Informatics (*in Greek*), p. 256.

#### **4. The dictates of the Law No. 3471/2006 about personal data e-processing**

##### ***a. Personal data processing principles in the publicly available electronic communications services***

The keynote principles, which are provided by the Law No. 2472/1997 for the protection of personal data and privacy can govern the personal data processing in the field of electronic communications as well, on condition that they are modified appropriately. Therefore, in the digital environment the principle of lawful method of data collection<sup>20</sup> dictates that the personal data of electronic communications' users or subscribers should be collected fairly and lawfully and the principle of scope<sup>21</sup> provides that these data should be collected for specified, explicit and legitimate purposes and should not be further processed in a way incompatible with those purposes<sup>22</sup>. The aforementioned data should, also, be accurate, true, and –where necessary– kept up to date, according to the principle of accuracy<sup>23</sup>. Additionally, the Law No. 3471/2006 restates the principle of necessity, particularizes the principle of finite data retention duration and specifies the features of the data subject's consent to the processing of his/her personal data in the digital networks<sup>24</sup>, as follows:

##### **i. Principle of necessity**

According to the principle of necessity, which is formulated in the Law No. 2472/1997, the personal data should be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.<sup>25</sup> Virtually, this principle is a specialization of the principle of proportionality.<sup>26</sup>

---

20. See P. Armamentos/V. Sotiropoulos (2005), *Personal Data – Commentary of the Law No. 2472/1997 (in Greek)*, p. 115. See, also, article 4 § 1 (a) of the Law No. 2472/1997 and article 6 § 1 (a) of the Directive 95/46/EC.

21. See P. Armamentos/V. Sotiropoulos (2005), *Personal Data – Commentary of the Law No. 2472/1997 (in Greek)*, p. 117.

22. See article 4 § 1 (a) of the Law No. 2472/1997 and article 6 § 1 (b) of the Directive 95/46/EC.

23. See P. Armamentos/V. Sotiropoulos (2005), *Personal Data – Commentary of the Law No. 2472/1997 (in Greek)*, p. 130. See, also, article 4 § 1 (c) of the Law No. 2472/1997 and article 6 § 1 (d) of the Directive 95/46/EC.

24. See the preamble of the Law No. 3471/2006 in the legal database [www.dsanet.gr](http://www.dsanet.gr).

25. See article 4 § 1 (b) of the Law No. 2472/1997 and article 6 § 1 (c) of the Directive 95/46/EC.

26. See P. Armamentos/V. Sotiropoulos (2005), *Personal Data – Commentary of the Law No. 2472/1997 (in Greek)*, p. 123.

The principle of necessity of personal data processing occurs also in the Law No. 3471/2006 in a harsher phrasing.<sup>27</sup> Under this principle, personal data processing should be restricted to the extent that is absolutely necessary for the sort and the purpose of the processing<sup>28</sup>. Moreover, the providers of publicly available electronic communications services must take the appropriate technical measures and must design and select the appropriate information systems in order to process the absolutely necessary personal data.<sup>29</sup>

We should, also, point out that the article 5 § 7 of the Law No. 3471/2006, as it was amended by the article 8 of the Law No. 3783/2009, obliges the providers of publicly available electronic communications services to render *the payment* for these services possible anonymously or pseudonymously, if it is technically feasible (e.g. with a prepaid card<sup>30</sup> for a specific duration of calls). Nevertheless, concerning *the use* of these services, the article 3 § 1 of the Law No. 3783/2009 provides that the users or subscribers must state solemnly the personal data, which are mentioned to the article 2 § 4 of the aforementioned Law<sup>31</sup>, to the providers of publicly available electronic communications services. This legislative regulation aims at the protection of national security and the prevention, investigation, detection and prosecution of criminal offences, terroristic actions and organized crime by the prosecuting authorities.<sup>32</sup> It is a fact that anonymity in the field of electronic communications contributes to the protection of users' and subscribers' right to informational self-determination.<sup>33</sup> However, the undoubt-

---

27. Compare to V. Tountopoulos, Protection of personal data in the field of telecommunications – The implementation of the Directive 97/66 in the Greek legislation (*in Greek*), Dikaio Epixeiriseon & Etaireion 5/2000, 479.

28. See article 5 § 1 of the Law No. 3471/2006.

29. See article 5 § 6 of the Law No. 3471/2006.

30. According to the 13<sup>th</sup> recital of the preamble of the Directive 2002/58/EC, prepaid cards are considered as a contract.

31. An individual must state his name, surname, father's name, place and date of birth and taxpayer's identification number to the network service providers and deposit to them a copy of his identity card. Respectively, a legal entity must state its firm, the address of its central offices, its taxpayer's identification number, as well as the name, surname and father's name of its legal representative.

32. See the preamble of the Law No. 3783/2009 in the legal database [www.dsanet.gr](http://www.dsanet.gr).

33. See Gr. Lazarakos, Anonymity and Internet (*in Greek*), Dikaio Meson Enimerosis & Epikoinonias 2/2005, 199.

edly respectable right to anonymity should not give rise to the impunity of criminal offenders.<sup>34</sup>

## ii. Principle of finite data retention duration

According to the Law No. 2472/1997, personal data must be kept in a form, which renders the identification of data subjects possible up to the end of the period that is necessary for the purposes for which the data were collected or for which they are further processed.<sup>35</sup> This principle of finite data retention duration is further specified in the Law No. 3471/2006. So, subscribers' or users' traffic data, which are being processed and stored by the provider of a publicly available communications service, must be erased or made anonymous when it is no longer needed for the purpose of the processing.<sup>36</sup> Consequently, traffic data processing for the purpose of the conveyance of a communication is permissible only up to the end of each communication<sup>37</sup> and traffic data processing for the purposes of subscriber billing and interconnection payments is permissible only up to the end of the period during which the bill may be challenged lawfully or payment may be pursued<sup>38</sup>, namely for the fulfillment of the contract<sup>39</sup>. As to location data, their processing is permissible to the extent and for the duration necessary for the provision of a value added service on condition that they are made anonymous with the appropriate codification or the service providers obtain the user's or subscriber's consent to the processing, after informing them about the type of location data which will be processed, about the purposes and duration of processing and about the eventual transmission of the data to a third party for the purpose of providing the value added service. In the latter case, users or subscribers should be given the possibility to withdraw their consent whenever and should have the opportunity to object to the processing of location data temporarily, free of charge and on the occasion of each connection to the network and each transmission of a communication.<sup>40</sup> Exceptionally, location data processing

---

34. See *M. Stathopoulos*, The use of personal data and the struggle between the rights of their controllers and the rights of their data subjects (*in Greek*), *Nomiko Vima* 2000, 9 · *Gr. Lazarakos*, Anonymity and Internet (*in Greek*), *Dikaio Meson Enimerosis & Epikoinonias* 2/2005, 199.

35. See article 4 § 1 (d) of the Law No. 2472/1997.

36. See article 6 § 1 of the Law No. 3471/2006 and article 6 § 1 of the Directive 2002/58/EC.

37. See articles 4 § 4 and 6 § 1 of the Law No. 3471/2006. See, also, articles 5 § 1 and 6 § 1 of the Directive 2002/58/EC.

38. See article 6 § 2 of the Law No. 3471/2006 and article 6 § 2 of the Directive 2002/58/EC.

39. See article 5 § 2 (b) of the Law No. 3471/2006.

40. See article 6 § 3 of the Law No. 3471/2006 and article 9 §§ 1-2 of the Directive 2002/58/EC.

is permitted without the user's or subscriber's consent for the purpose of facing an emergency case.<sup>41</sup>

However, it must be stressed that the Law No. 3917/2011, which brings into force the regulations of the Data Retention Directive (Directive 2006/24/EC) in the Greek law and order, dictates that the providers of publicly available electronic communications services or of a public communications network must retain the external data of an electronic communication for a period of twelve (12) months from the date of the communication to the extent that those data are generated or processed by them (the providers) within their jurisdiction in the process of supplying the communications services concerned<sup>42</sup>. So, the above recent Law redefines the retention period of the external data of an electronic communication by stretching the Law No. 3471/2006, and renders access to these data possible for the national authorities for the purposes of investigation, detection and prosecution of serious crimes<sup>43</sup>. The result of this recent legislative regulation is the dwindling of the protection, which the Law No. 3471/2006 provides in relation to the aforementioned data.<sup>44</sup>

### **iii. Users' or subscribers' consent as a prerequisite for lawful processing of their personal data**

Users or subscribers of electronic communications services are mostly ignorant of the fact that, when they browse the web, they make legal transactions, such as consent to their personal data processing.<sup>45</sup> This consent leads to a shrinkage of users' and subscribers' private sphere<sup>46</sup> and is usually given in return for the provision of free information in the internet<sup>47</sup>. If the data subject does not consent to

---

41. See article 6 § 4 of the Law No. 3471/2006 and article 10 of the Directive 2002/58/EC.

42. See articles 3 and 6 of the Law No. 3917/2011 and articles 3 and 6 of the Directive 2006/24/EC. The obligation to retain the external data of an electronic communication includes the retention of these data relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by the providers of publicly available electronic communications services or of a public communications network in the process of supplying the communication services concerned.

43. See article 4 of the Law No. 3917/2011 and article 4 of the Directive 2006/24/EC.

44. Compare to I. Igglezakis (2008), *Law of Informatics (in Greek)*, p. 265.

45. See G. Georgiades (2003), *The contracting of an agreement via Internet (in Greek)*, pp. 29-30.

46. See G. Nouskalis (2004), *The penal protection of digital information (in Greek)*, in: *Digital Technology and Law – Union of Jurists of Northern Greece*, vol. 52, p. 164.

47. See G. Georgiades (2003), *The contracting of an agreement via Internet (in Greek)*, p. 30 · I. Igglezakis, *The protection of personal data in the Internet – Regulations of national and community Law (in Greek)*, Episkopisi Emporikou Dikaiou 2002, 683.



the processing of his/her personal data, his/her access to the information super-highways is not feasible.<sup>48</sup>

Consent is any freely given, explicit, specific and informed indication of wishes by which the data subject signifies his agreement to the processing of his personal data.<sup>49</sup> It is a unilateral legal transaction<sup>50</sup> that is addressed to the data controller, who is mostly the provider of publicly available electronic communications services. Data subject's consent has the following special characteristics:

- a. It must be given freely. So, the user or subscriber must be able to decide on whether he will give his consent or not. At all events, consent must not be given under conditions of mental or physical violence<sup>51</sup>, deception, fraud or threat, and must not contravene the statute and moral law<sup>52</sup>.
- b. It must be explicit and unambiguous on the grounds that it is of major importance for personal data protection.<sup>53</sup> Tacit consent is not valid.<sup>54</sup>
- c. It must be specific, namely it must be given for a specific purpose and it must not cover in advance any future processing.<sup>55</sup> So, if the users or subscribers give their consent for any processing of their personal data without restrictions for the data retention period, the type of processing and the recipients to whom the data might be disclosed, this consent is not valid.<sup>56</sup>

48. See G. Nouskalis (2004), The penal protection of digital information (*in Greek*), in: Digital Technology and Law – Union of Jurists of Northern Greece vol. 52, p. 164.

49. See article 2 of the Law No. 2472/1997 and article 5 §§ 2-4 of the Law No. 3471/2006.

50. See F. Doris, in: Civil Code Georgiades/Stathopoulos (*in Greek*), art. 236, section 10.

51. See G. Georgiades, The Law No. 3471/2006 about the protection of privacy in electronic communications (*in Greek*), *Chronika Idiotikou Dikaiou* 2007, 22.

52. See K. Christodoulou, To a re-examination of the meaning of the legal transaction? The paradigm of data subject's consent to his personal data processing (*in Greek*), *Dikaio Meson Enimerosis & Epikoinonias* 3/2005, 359 · E. Alexandropoulou-Egyptiadou (2007), Personal Data (*in Greek*), p. 45.

53. Compare to V. Tountopoulos, Protection of personal in the field of telecommunications – The implementation of the Directive 97/66 in the Greek legislation (*in Greek*), *Dikaio Epixeiriseon & Etaireion* 5/2000, 479.

54. Compare to I. Igglezakis (2004), Sensitive personal data (*in Greek*), p. 218.

55. See K. Christodoulou, To a re-examination of the meaning of the legal transaction? The paradigm of data subject's consent to his personal data processing (*in Greek*), *Dikaio Meson Enimerosis & Epikoinonias* 3/2005, 361 · E. Alexandropoulou-Egyptiadou (2007), Personal Data (*in Greek*), p. 60.

56. Compare to I. Igglezakis (2004), Sensitive personal data (*in Greek*), pp. 220 and 222.

d. Data controller is obliged to provide the user or subscriber with clear information about the categories of personal data, the purpose of the processing and the recipients or categories of recipients to whom the data might be disclosed as well.<sup>57</sup> The user or subscriber must, also, be informed about the name and the address of the controller and of his representative and the proposed transfers of data to third countries<sup>58</sup>. The notification must be easily comprehensible, true, clear and complete, namely must contain both positive and negative effects of the processing.<sup>59</sup> Usually, the above information are included to the text of Privacy Policy of the website of a provider of electronic communications services.<sup>60</sup> Consent, which is given without prior adequate notification, is void, because it does not provide guarantees for the free expression of the user's or subscriber's will.<sup>61</sup>

It must be stressed that, though the Directive 2002/58/EC makes no provision for compliance with legal formalities about the data subject's consent for his personal data processing<sup>62</sup>, the article 5 § 3 of the Law No. 3471/2006 provides that user's or subscriber's consent to the processing of his/her personal data must be given either through a document, which bears the data subject's handwritten signature or by "*electronic means*"<sup>63</sup>, namely through an electronic document. However, it is not required for the electronic document to bear the advanced electronic signature, which would equate an electronic document with a document that bears a handwritten signature.<sup>64</sup> So, consent may be given on-line by any proper means that guarantees the free and informed expression of user's or subscriber's will. Therefore, consent may be given electronically, even by ticking a box

---

57. See article 5 § 2 of the Law No. 3471/2006.

58. Compare to I. Igglezakis (2004), Sensitive personal data (*in Greek*), p. 220. See, also, article 2 of the Law No. 2472/1997.

59. See Gr. Lazarakos, Creation of Websites and personal data protection (*in Greek*), Dikaio Meson Enimerosis & Epikoinonias 4/2005, 553-554.

60. See I. Igglezakis (2004), Sensitive personal data (*in Greek*), p. 222.

61. See K. Christodoulou, To a re-examination of the meaning of the legal transaction? The paradigm of data subject's consent to his personal data processing (*in Greek*), Dikaio Meson Enimerosis & Epikoinonias 3/2005, 358 · I. Igglezakis (2004), Sensitive personal data (*in Greek*), p. 220.

62. See K. Christodoulou (2006), Protection of personality and contractual freedom in public available networks (*in Greek*), p. 107.

63. See K. Christodoulou (2006), Protection of personality and contractual freedom in public available networks (*in Greek*), p. 104.

64. See K. Christodoulou (2006), Protection of personality and contractual freedom in public available networks (*in Greek*), p. 104.

when browsing a website (mouse-click consent).<sup>65</sup> At all events, the user's and subscriber's consent must be embodied permanently in a stable storage device, so that it is easy of access to him/her<sup>66</sup> and the data controller will be able in the future to prove the receiving of the consent.<sup>67</sup> If data controller obtains consent without being observant to the abovementioned legal formalities, the consent is void, according to the article 159 of the Greek Civil Code.

We should, also, emphasize that consent must be given in writing, if personal data are disclosed to third parties<sup>68</sup>. Providers of publicly available electronic communications services are not supposed to be third parties, regarding the traffic data transmission to them by another corresponding provider with the sole purpose of billing of the services, on condition that the user or subscriber has been informed in writing before the drawing up of the agreement.<sup>69</sup>

Eventually, the data subject has the right to withdraw his consent.<sup>70</sup> The withdrawal of this consent is a unilateral legal transaction, which is addressed to the controller and, according to the article 164 of the Greek Civil Code, is subject to consent's legal formalities.<sup>71</sup> In advance renunciation of the user's or subscriber's right to withdraw his consent is void, because it amounts to a blank consent to the processing of his personal data for any purpose in the future.<sup>72</sup>

---

65. See the 17<sup>th</sup> recital of the preamble of the Directive 2002/58/EC. Also, see Korn. Delouka-Igglesi, Consumer's protection from the direct advertisement in the internet (*in Greek*), Dikaio Meson Enimerosis & Epikoinonias 4/2004, 496 · An. Spiliotopoulou/I. Chochliouros, Lawful interception of communications while ensuring individual's privacy (*in Greek*), Nomiko Vima 2007, 1961. Referring to the term "mouse-click consent", it occurs in: L. Mitrou (2005), Self-regulation in the Cyberspace (*in Greek*), in: Th. K. Papachristou/ Ch. Vernardakis/ G. Theodosis/ If. Kamtsidou/ K. Manolakou/ L. Mitrou/ V. Papakonstantinou/ E. Rethimiotaki/ K. Stratilati/G. Tasopoulos, Self-regulation, Law & Society in the 21<sup>st</sup> Century, vol. 9, p. 85.

66. See article 5 § 3 of the Law No. 3471/2006.

67. See K. Christodoulou (2006), Protection of personality and contractual freedom in public available networks (*in Greek*), p. 105.

68. For the meaning of the term "third party" see article 2 of the Law No. 2472/1997 and article 2 (f) of the Directive 95/46/EC.

69. See article 5 § 5 of the Law No. 3471/2006.

70. See article 5 § 3 of the Law No. 3471/2006.

71. See F. Doris, in: Civil Code Georgiades/Stathopoulos (*in Greek*), art. 237, section 5.

72. See K. Christodoulou, To a re-examination of the meaning of the legal transaction? The paradigm of data subject's consent to his personal data processing (*in Greek*), Dikaio Meson Enimerosis & Epikoinonias 3/2005, 363.

***b. The protection of the confidentiality of communications in the digital networks***

According to the article 4 § 1 of the Law No. 3471/2006, the use of electronic communications services, which are provided by means of a public communications network and publicly available electronic communications services, as well as the related traffic data and location data, are protected as confidential. Consequently, listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data and location data is prohibited<sup>73</sup>, except from the cases that is permitted by the Greek legislation for the purposes of protection of national security or detection of serious crimes.

However, technical storage of data, which are necessary for the conveyance of a communication is permitted without prejudice to the principle of confidentiality.<sup>74</sup> Technical storage is, also, lawful, if it is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user, on condition that the subscriber or user concerned is provided with clear and comprehensive information about the purposes of the processing and is offered the right to refuse such processing by the data controller.<sup>75</sup>

Traffic data, which are necessary for the purposes of subscriber billing and inter-connection payments, may be processed lawfully by the provider of electronic communications services without the subscriber's prior consent<sup>76</sup>, just because it is required for the fulfillment of the contract<sup>77</sup>. Such processing is permissible only up to the end of the period during which the bill may be lawfully challenged or payment may be pursued<sup>78</sup>, as the purpose of the processing is the proof of the subscriber's debt. For example, the provider of a mobile network keeps legally a record of the home addresses of his subscribers, because it is necessary for the billing of the services and the dispatch of the bill. However, in the case of prepaid mobile services the processing of these data is not a prerequisite for the fulfillment of the contract, because the price for the services is prepaid, when the

---

73. See article 4 § 2 of the Law No. 3471/2006 and article 5 § 1 of the Directive 2002/58/EC.

74. See article 4 § 4 of the Law No. 3471/2006 and article 5 § 1 of the Directive 2002/58/EC.

75. See article 4 § 5 of the Law No. 3471/2006 and article 5 § 3 of the Directive 2002/58/EC.

76. See article 6 § 2 of the Law No. 3471/2006 and article 6 § 2 of the Directive 2002/58/EC.

77. See article 5 § 2 of the Law No. 3471/2006.

78. See article 6 § 2 of the Law No. 3471/2006 and article 6 § 2 of the Directive 2002/58/EC.

user buys the card and, thereupon, there is no question of payment or the bill is beyond dispute.<sup>79</sup>

We should, also, mention that the digital networks and the mobile telecommunications networks offer to the called subscriber the possibility of presentation of the calling line identification before the beginning of a communication<sup>80</sup>. As an offset to this possibility the article 8 § 1 of the Law No. 3471/2006 dictates that the calling user should be able to prevent the presentation of the calling line identification on a per-call basis using a simple means and free of charge. The calling subscriber is offered this possibility on a per-line basis. However, the possibility of preventing the presentation of the calling line identification of incoming calls must not become an obstacle to the detection of malicious<sup>81</sup> or nuisance<sup>82</sup> calls or to the handling of emergency calls. Therefore, traffic data and location data of users and subscribers of publicly available electronic communications services may, also, be processed without their consent in the aforementioned cases.<sup>83</sup> Consequently, the providers of publicly available electronic communications services must take the appropriate technical measures in order to render it possible to override: a. the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls, and b. the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organizations dealing with emergency calls for the purpose of responding to such calls.<sup>84</sup>

---

79. See *Gr. Tsolias*, Personal data in the field of electronic communications and “reverse search” of them for the purpose of detection of very serious crimes – On the occasion of No. 19/2008 Decision of the Greek Data Protection Authority (*in Greek*), *Dikaio Meson Enimerosis & Epikoinonias* 2/2008, 178.

80. See *L. Mitrou*, The new Directive 2002/58/EC for the protection of privacy in electronic communications, *Dikaio Meson Enimerosis & Epikoinonias* 3/2004, 374.

81. Malicious call is the call, which poses a threat of violence/compulsion or other unlawful act or failure, insult, affront to sexual dignity or extortion. For the meaning of the term “malicious call” see article 2 of the act No. 2322/11.12.2006 of the Hellenic Authority for Communication Security and Privacy.

82. Nuisance call is the call, which disturbs domestic peace and causes anxiety (e.g. silent and repeated calls). For the meaning of the term “nuisance call” see article 2 of the act No. 2322/11.12.2006 of the Hellenic Authority for Communication Security and Privacy.

83. See article 8 § 7 of the Law No. 3471/2006.

84. See article 8 § 7 of the Law No. 3471/2006 and article 10 of the Directive 2002/58/EC. The elimination of the presentation of calling line identification may be overridden: a. upon application of a subscriber requesting the tracing of malicious or nuisance calls, and b. for the purpose of dealing with emergency calls, under the requirements of the acts No.

Finally, regarding the recording of electronic communications and the related traffic data, it is permissible when it is carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication on condition that both parties give their “informed consent”.<sup>85</sup> On the contrary, if the abovementioned recording takes place without the consent of the parties, it is a breach of confidentiality of the communications and, therefore, it is prohibited.

### ***c. The unsolicited electronic communications***

The unsolicited electronic communications, namely the processing of the users’ or subscribers’ traffic data -mostly without their prior consent- for the purposes of direct marketing of products or services, is very common nowadays. These unsolicited electronic communications are carried out by means of automated calling systems *with or without* human intervention, facsimile machines (fax), electronic mail or via mobile networks.

The Greek legislator regulates the unsolicited electronic communications for the purposes of direct marketing with the article 11 of the Law No. 3471/2006. According to this article, the unsolicited electronic communications for the purposes of direct marketing, which is carried out by the abovementioned ways, are permitted only in respect of subscribers who have given their prior consent. The same rule applies to individuals and legal entities as well.<sup>86</sup>

Exceptionally, if an individual or legal entity obtains from its customers their electronic contact details, in the context of the sale of a product or a service, the same individual or legal entity may use these electronic contact details for direct marketing of its own similar products or services, on condition that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of their electronic contact details and on the occasion of each message in case the customer has not initially refused such use.<sup>87</sup> In addition, the practice of sending electronic mail for the purpose of direct marketing disguising or concealing the identity of the sender on whose behalf the communi-

---

2322/11.12.2006 and 2002/3.9.2008 of the Hellenic Authority for Communication Security and Privacy.

85. See article 4 § 3 of the Law No. 3471/2006 and article 5 § 2 of the Directive 2002/58/EC.

86. In relation to these regulations see article 11 §§ 1 and 5 of the Law No. 3471/2006.

87. See article 11 § 3 of the Law No. 3471/2006 and article 13 § 2 of the Directive 2002/58/EC.

cation is made, or without a valid address to which the recipient may request the cessation of such communications, is prohibited.<sup>88</sup>

Article 11 § 2 of the Law No. 3471/2006 regulates each provider of publicly available electronic communications services to keep an e-Robinson register, in which all the declarations of subscribers, who do not desire to receive unsolicited electronic communications for the purpose of direct marketing, will be recorded free of charge. Everyone, who proceeds to such communications, must refer regularly to these e-Robinson registers and must not disturb the subscribers, who are enrolled to them.<sup>89</sup>

The above rules adopt the system of prior consent for all the unsolicited electronic communications *with or without* human intervention parallel to the duty of the providers of publicly available electronic communications services to keep the e-Robinson register. However, this legal regulation contravenes the article 13 of the Directive 2002/58/EC for the following reason: The first paragraph of this article dictates that the use of automated calling systems *without* human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be permitted in respect of subscribers, who have given their prior consent. However, regarding the cases of unsolicited electronic communications *with* human intervention, the third paragraph of the above article dictates that Member States shall take appropriate measures to ensure that they are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation. So, the present regulation of the article 11 § 1 of the Law No. 3471/2006 renders ineffective the article 11 § 2 of the same Law, because at all events prior consent of the user or subscriber is essential so that the unsolicited electronic communications are lawful<sup>90</sup>.

In order to remove this contradictory regulation, the Greek legislator has already instituted the article 16 of the recent Law No. 3917/2011, which amends the aforementioned rules and takes effect on 1.9.2011<sup>91</sup>. According to this amendment, the unsolicited electronic communications for the purposes of direct mar-

---

88. See article 11 § 4 of the Law No. 3471/2006 and article 13 § 4 of the Directive 2002/58/EC.

89. See Korn. Delouka-Igglesi, Consumer's protection from the direct advertisement in the internet (in Greek), Dikaio Meson Enimerosis & Epikoinonias 4/2004, 496.

90. See the preamble of the Law No. 3917/2011 in the website <http://www.ministryofjustice.gr/site/LinkClick.aspx?fileticket=In68q5jddW0%3d&tabid=132>.

91. See article 16 § 3 of the Law No. 3917/2011.

keting which are carried out by means of automated calling systems *without* human intervention, facsimile machines (fax) and electronic mail are permitted only with the prior consent of the user or subscriber. On the contrary, the unsolicited electronic communications for the above purposes, which are carried out by means of automated calling systems *with* human intervention, are prohibited, if the subscriber has declared to the provider of a publicly available electronic communications service that he/she does not want to receive such calls.

## 5. Conclusion

The regulations of the Law No. 3471/2006, as it is amended, specify the conditions under which the processing of the personal data of users or subscribers of electronic communications is lawful and legitimate. So, these regulations set clear and distinct limits to the personal data e-processing by virtue of the needs and risks arising from the rapid development of the digital networks and, therefore, function as precautionary measures of personal data protection in the digital environment. If the personal data e-processing does not meet the requirements of the above Law without prejudice to the Greek legislative regulations, which put aside the confidentiality of the electronic communications, as well as the related traffic data and location data, for the purposes of protection of public safety and detection of serious crimes, it is illegal and gives rise to legal claims on the side of the harmed user or subscriber of electronic communications services.



# **The Budapest's Convention as a guarantee limit against cybercrime**

---

---

**Eleni Chrysopoulou**

---

---

## **1. Introduction**

The vertiginous growth of the Internet has dramatically changed the way entities interact. Cyberspace enables people to share ideas over great distances and engage in the creation of an entirely new, diverse and chaotic democracy, free from geographic and physical constraints [Aldesco I.A., 2002]. The rapid progress of information technology has achieved significant advances in processing and transmitting data through use of computers and computer networks resulting in substantial benefits to society, including the ability to communicate with others real-time, access a library of information and transmit data instantly [Hopkins L.S., 2003].

The dark side of the above phenomenon is the fostering of new kinds of crimes, additional means to commit existing crimes and increased complexities of prosecuting crimes, since historical obstacles to international crime, such as distance, time and space, have now been eliminated. This international element in the commission of crime, whether it be traditional or new technological computer crime, creates new problems for both legal policy and law enforcement.

The above described challenge resulted in the Budapest's Convention, which with respect to human rights, aims at the adoption of appropriate and adequate international legal measures by the contracting countries.

The Convention on cybercrime provides a treaty-based framework that imposes on the participating nations the obligation to enact legislation criminalizing certain conduct related to computer systems, create investigative procedures and ensure their availability to domestic law enforcement authorities to investigate cybercrime offenses, including procedures to obtain electronic evidence in all of its forms and create a regime of broad international cooperation, including assistance in extradition of fugitives sought for crimes identified under the Convention [Marshall J.J., 2005].

## 2. The Cybercrime Convention

### 2.1 *Importance of the Convention*

A treaty, according to Article 2 of Vienna Convention, is “an international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation” [Council of Europe]. Treaties are the only machinery that exist for adapting international law to new conditions and strengthening the force of a rule of law between states [Brierly J.L., 1963]. Thus, and taking into account the Council’s of Europe declaration of the need to pursue a common criminal policy aimed at the protection of the society against cybercrime [Preamble, par.4], it seemed very important for an international regime to be set up to combat these types of crimes in a growing and integrated global society.

### 2.2 *The way to the Convention*

Before the Budapest’s Convention adoption, a number of Committee of Ministers Recommendations’ had been issued in an attempt to combat cybercrime. These Recommendations, also mentioned in the Convention’s Preamble, are Committee of Ministers Recommendations No. R (85) 10, concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2, on piracy in the field of copyright and neighbouring rights, No. R (87) 15, regulating the use of personal data in the police sector, No. R (95) 4, on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9, on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13, concerning problems of criminal procedural law connected with information technology.

The Council of Europe’s Convention on Cybercrime and its Explanatory Report have been adopted by the Committee of Ministers of the Council of Europe at its 109th Session on November 8, 2001 and the Convention was opened for signature on November 23, 2001.

Negotiations on the Convention began in 1997, following a determination by the Council that the transnational character of cybercrime could only be tackled at the global level. To date, the Convention has been signed by 43 Council of Europe members and four non-members (Canada, Japan, South Africa and the United States) that also participated in the negotiations [Appendix]. It has also been sup-

plemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence.

Greece signed the Convention on 23.11.2001, but has yet to ratify it. Although, some provisions of the Convention are already covered by existing Greek domestic legislation, there still is a long way ahead. The distance will be covered with the Convention's critical and careful incorporation into the Greek legal order.

### ***2.3 Objectives of the Convention***

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

As recognized in the Convention's Preamble, the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks and the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks, require co-operation between States and private industry in combating cybercrime and increased, rapid and well-functioning international co-operation in criminal matters.

Moreover, the Council of Europe is mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties and also mindful of the right to the protection of personal data.

The Convention, as it is declared in its explanatory report, aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation [Explanatory Report, par.16].

Thus, the Convention's main goal is to establish a "common criminal policy" to better combat computer-related crimes worldwide through harmonizing national legislation, enhancing law enforcement and judicial capabilities, and improving international cooperation. To these ends, the Convention is broken up into four

main chapters: The first chapter defining the terms to be used, the second chapter referring to the measures to be taken at the national level, containing substantive law, procedural law and jurisdiction measures, the third chapter referring to the international cooperation and the fourth chapter, regarding the final provisions of the Convention.

## **2.4 The definitions of the Convention**

Article 1 initially defines four terms vital to the treaty. The first term defined is “computer system”, which is a device consisting of hardware and software developed for automatic processing of digital data [Explanatory Report, par.23]. For the purposes of this Convention, the definition of “computer data” builds upon the ISO-definition of data and must be in a form suitable for processing in a computer system [Explanatory Report, par.25]. The term “service provider” encompasses a broad category of persons that play a particular role with regard to communication or processing of data on computer systems. This definition includes both public or private entities and “those entities that store or otherwise process data on behalf of public or private entities” [Explanatory Report, par. 26, 27]. The fourth defined term is “traffic data” which means data that is generated by computers in the chain of communication in order to route a communication from its origin to its destination. It is therefore auxiliary to the communication itself. When a Convention Party investigates a criminal offence within this treaty, traffic data is used to trace the source of the communication. Traffic data lasts for only a short period of time and the Convention makes Internet Service Providers (ISPs) responsible for preservation of this data [Explanatory Report, par. 28-31].

It is noted that Convention Parties would not be obliged to copy *verbatim* into their domestic laws the four concepts defined in Article 1, provided that these laws cover such concepts in a manner consistent with the principles of the Convention and offer an equivalent framework for its implementation [Explanatory Report, par.22].

## **3. Substantive law issues**

Although there is an internationally continuing discussion “on just what constitutes a computer crime”, there is yet no generally accepted definition of the term. The Convention on cybercrime supports this effort to define computer crime by including an array of different computer related offences in its substantive criminal law provisions [Viano C.E., 2004].

### ***3.1 Confidentiality, integrity and availability offences***

The purpose of this section of the Convention (Section 1, Articles 2-13) is to establish a common minimum standard of relevant offences so as to improve the means to prevent and suppress computer- or computer-related crime. Correspondence in domestic law may prevent abuses from being shifted to a Party with a previous lower standard. As a consequence, the exchange of useful common experiences in the practical handling of cases may be enhanced, too [Explanatory Report, par.33].

As stated in the Explanatory Report, All the offences contained in the Convention must be committed “intentionally” for criminal liability to apply. In certain cases an additional specific intentional element forms part of the offence. The drafters of the Convention agreed that the exact meaning of ‘intentionally’ should be left to national interpretation [Explanatory Report, par.39].

The criminal offences in Articles 2-6 were intended by the drafters to protect the confidentiality, integrity and availability of computer systems or data and not to criminalise legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices [Explanatory Report, par.43].

#### **Illegal access**

“Illegal access” covers the basic offence of dangerous threats to and attacks against the security, meaning the confidentiality, integrity and availability of computer systems and data. Examples of unauthorised acts of intrusion, which should be in principle illegal are “hacking”, “cracking” or “computer trespass”. Such intrusions may give access to confidential data, like passwords, information about the targeted system and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.

The act must also be committed “without right”, meaning that there is no criminalisation of the access authorised by the owner or other right holder of the system or part of it, such as for the purpose of authorised testing or protection of the computer system concerned [Explanatory Report, par. 44, 47].

#### **Illegal interception**

This provision aims to protect the right of privacy of data communication. The offence which is criminalized is the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The provision is based upon the right to privacy of correspond-

ence of the Article 8 of the European Convention on Human Rights and the offence of “unauthorised interception” described in Recommendation (89) 9. The offence established at this point applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer and applies to ‘non-public’ transmissions of computer data. The term ‘non-public’ qualifies the nature of the transmission process and not the nature of the data transmitted, meaning that the data communicated may be publicly available information, but the parties wish to communicate confidentially or data may be kept secret for commercial purposes until the service is paid, as in Pay-TV. For criminal liability to attach, the illegal interception must be committed “intentionally”, and “without right” [Explanatory Report, par. 51, 52, 54, 58].

### **Data interference**

The acts of damaging, deletion, deterioration, alteration or suppression of computer data is, under this provision, punishable, if committed without right in a way that computer data and computer programs are protected the same way to that enjoyed by corporeal objects against intentional infliction or damage. The offender, here, must have acted “intentionally”, too [Explanatory Report, par. 60, 63].

### **System Interference**

The criminalization of the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data is based upon the “computer sabotage” of the Recommendation No. (89)9. The “hindering” must be “without right” and “serious” and the offence must be committed “intentionally” in order to give rise to criminal sanction [Explanatory Report, par. 65, 67, 68, 70].

### **Misuse of devices**

This article establishes, as separate and independent offences, the intentional commission of illegal acts regarding certain devices that are used in the commission of the named offences of this Convention. The article intends to combat black markets which are established to facilitate the sale or trade of “hacker tools,” or tools used by hackers in the commission of cybercrimes by prohibiting the production, sale, or distribution of these devices. The drafters intended this Article to relate to devices that “are objectively designed, or adapted, primarily for the purpose of committing an offence”. Finally, in order to avoid overcriminalization, Article 6 requires both a general intent and also a “specific... intent that the device is used for the purpose of committing any of the offences established in Articles 2-5 of the Convention” [Explanatory Report, par. 71, 72, 73, 76].

### ***3.2 Computer-related offences***

The purpose of Article 7, which outlaws computer-related forgery, is to create a parallel offence to the forgery of tangible documents. It is also noted that national concepts of forgery vary greatly, but, it was agreed that the deception as to authenticity refers at minimum to the issuer of the data, regardless of the correctness or veracity of the contents of the data. Parties may go further and include under the term “authentic” the genuineness of the data, if they choose so [Explanatory Report, par. 81, 82].

Article 8 makes computer-related fraud illegal. The aim of this article is to criminalise any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property and its objective is to protect assets represented or administered in computer systems, such as electronic funds and money deposits. The computer fraud manipulations are criminalised if they are committed “intentionally”, “without right” and moreover, produce a direct economic or possessory loss of another person’s property and the perpetrator acted with the intent of procuring an unlawful economic gain for himself or for another person [Explanatory Report, par. 86, 89, 90].

### ***3.3 Content-related offences***

Article 9 tries to strengthen and modernize the existing criminal law provisions against sexual exploitation of children and expand them to electronic transmissions. The described illicit acts related to child pornography must be criminalized by the Parties if committed “intentionally”.

This provision responds to the preoccupation of Heads of State and Government of the Council of Europe, expressed at their 2nd summit (Strasbourg, 10 – 11 October 1997) in their Action Plan (item III.4) and corresponds to an international trend that seeks to ban child pornography, as evidenced by the recent adoption of the Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child prostitution and child pornography and the recent European Commission initiative on combating sexual exploitation of children and child pornography (COM2000/854).

It criminalises various aspects of the electronic production, possession and distribution of child pornography to combat the new form of sexual exploitation and endangerment of children via the internet. Paragraph 1(a) criminalises the production of child pornography for the purpose of distribution through a computer system, when paragraph 1(b) criminalises the “offering” of child pornography through a computer system and also intends to cover the creation or compilation of hyperlinks to child pornography sites in order to facilitate access to child por-

nography. Paragraph 1(c) criminalises the distribution or transmission of child pornography through a computer system, when in paragraph 1(d), actively obtaining child pornography, for example by downloading it, is criminalised. The possession of child pornography in a computer system or on a data carrier is criminalised in paragraph 1(e). [Explanatory Report, par. 91, 92, 94-98, 105]

The three types of pornographic material defined in paragraph 2 for the purposes of committing the offences contained in paragraph 1 cover depictions of sexual abuse of a real child (2a), pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct (2b), and finally images, which, although “realistic”, do not in fact involve a real child engaged in sexually explicit conduct (2c).

Paragraph 3 defines the term “minor” in relation to child pornography in general as all persons under 18 years, in accordance with the definition of a ‘child’ in the UN Convention on the Rights of the Child (Article 1). Nevertheless, the provision allows Parties to require a different age-limit, provided it is not less than 16 years [Explanatory Report, par. 94-102, 104].

### ***3.4 Infringements of copyright and related rights***

Infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet. Such protected works include literary, photographic, musical, audio-visual and other works. Each Party is obliged to criminalise wilful infringements of copyright and related rights, sometimes referred to as neighbouring rights, arising from the agreements listed in the article, when such infringements have been committed by means of a computer system and on a commercial scale. Copyright and related rights offences must be committed “wilfully” for criminal liability to apply. In contrast to all the other substantive law provisions of this Convention, the term “wilfully” is used instead of “intentionally” in both paragraphs 1 and 2, as this is the term employed in the TRIPS Agreement (Article 61), governing the obligation to criminalise copyright violations [Explanatory Report, par. 107, 108, 113].

### ***3.5 Attempt and aiding or abetting***

This article relates to offences dealing with intentionally attempting or aiding and abetting “the commission of the offences defined in the Convention”. Liability under Article 11 arises when “the person who commits a crime established in the Convention is aided by another who also intends that the crime be committed”. With respect to paragraph 2 on attempt, some offences defined in the Convention, or elements of these offences, were considered to be conceptually difficult to attempt, like for example, the elements of offering or making avail-



able of child pornography. According to the provision, it is only required that the attempt be criminalised with respect to offences established in accordance with Articles 3, 4, 5, 7, 8, 9(1)(a) and 9(1)(c) [Explanatory Report, par. 118-122].

### ***3.6 Corporate Liability***

Article 12 deals with the liability of legal persons. Here, liability is imposed on corporations, associations and similar legal persons for the criminal actions undertaken by a person in a leading position within such legal person, where undertaken for the benefit of that legal person. Article 12 also contemplates liability where such a leading person fails to supervise or control an employee or an agent of the legal person, where such failure facilitates the commission by that employee or agent of one of the offences established in the Convention. Under paragraph 1, four conditions need to be met for liability to attach, when under paragraph 2 Parties are obliged to have the ability to impose liability upon a legal person where the crime is committed not by the leading person described in paragraph 1, but by another person acting under the legal person's authority. Liability under this Article may be criminal, civil or administrative. Paragraph 4 clarifies that corporate liability does not exclude individual liability [Explanatory Report, par. 123-127].

### ***3.7 Sanctions and measures***

This provision requires that the Convention Parties provide criminal sanctions that are "effective, proportionate and dissuasive" and "include the possibility of imposing prison sentences" [Explanatory Report, par. 128].

## **4. Procedural law issues**

The Convention defines powers to facilitate criminal investigations.

### ***4.1 Scope of procedural provisions***

The articles in this section describe procedural measures that Convention parties must take "at the national level for the purpose of criminal investigation of the offences established in Section 1".

Electronic data may very well be the only evidence in a criminal investigation. One way in which the Convention overcomes the problem of the speed and the easiness that this evidence can be altered, moved, or deleted, is by adapting traditional procedures, like search and seizure, to an ever-changing technological landscape. However, in order to make these traditional crime investigation methods effective, new measures have been created, such as the expedited preserva-

tion of data, the real-time collection of traffic data, and the interception of content data [Explanatory Report, par. 131, 134].

#### ***4.2 Conditions and safeguards***

The establishment, implementation and application of the powers and procedures provided for in this Section of the Convention shall be subject to the conditions and safeguards provided for under the domestic law of each Party. Parties shall ensure that these conditions and safeguards provide for the adequate protection of human rights and liberties. The minimum safeguards to which Parties to the Convention must adhere include the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and its additional Protocols No. 1, 4, 6, 7 and 12 (ETS N°s 005, 009, 046, 114, 117 and 177), in respect of European States that are Parties to them and also, other applicable human rights instruments in respect of States in other regions of the world which are Parties to these instruments, as well as the more universally ratified 1966 International Covenant on Civil and Political Rights. In addition, there are similar protections provided under the laws of most States.

Another safeguard according to this article is that the powers and procedures shall “incorporate the principle of proportionality” [Explanatory Report, par. 145, 146].

Opponents to the Convention argue that the treaty infringes upon basic human rights and liberties, with the most significant of them to be, the right to privacy.

#### ***4.3 Expedited preservation of stored computer data***

Article 16 introduces a new measure in order to facilitate the investigation of cybercrimes. This measure, so as the other one referred in Article 17, apply to stored data, that has already been collected and stored at data holders and not to real time data. [Explanatory Report, par. 149].

Here, it has to be mentioned that while “data preservation” means keeping data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate, “data retention” means keeping data, which is currently being generated, in one’s possession into the future. On the one hand, data retention is the process of storing data. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe. Articles 16 and 17 refer only to data preservation, and not data retention [Explanatory Report, par. 151, 152].

Data preservation is for most countries an entirely new legal power or procedure in domestic law, as it is an important new investigative tool in addressing compu-

ter and computer-related crime, especially crimes committed through the Internet. The statute operates in either by the way in which the competent authorities in the Convention party country simply access, seize and secure the relevant data, or by the way in which, where a reputable business is involved, competent authorities can issue an order to preserve the relevant data. Convention parties are thus required to introduce a power that would enable law enforcement authorities to order the preservation of data for a particular period of time not exceeding 90 days. It is also noted that preservation measures exist at the national level in order to enable Parties to assist one another at the international level with expedited preservation of stored data located in their territory [Explanatory Report, par. 155-157].

#### ***4.4 Expedited preservation and partial disclosure of traffic data***

This article establishes specific obligations in relation to the preservation of traffic data under Article 16 and provides for expeditious disclosure of some traffic data so as to identify that other service. Obtaining stored traffic data that is associated with past communications may be critical in a criminal investigation. Article 17 ensures that where one or more service providers were involved in the transmission of a communication, expeditious preservation of traffic data can be effected among all of the service providers. Therefore, this article requires that the service provider, which receives a preservation order or similar measure, disclose expeditiously to the competent authorities, or other designated person, a sufficient amount of traffic data to enable the competent authorities to identify any other service providers and the path through which the communication was transmitted [Explanatory Report, par. 165-169].

#### ***4.5 Production order***

This provision relates to production orders, which specifically allow “competent authorities to compel a person in its territory to provide specified stored computer data” or to compel an Internet Service Provider to provide subscriber information. Article 18 relates exclusively to production of stored or existing data. Production orders precede search and seizure as a means of obtaining specific data. As the powers and procedures in this Section are for the purpose of specific criminal investigations or proceedings (Article 14), production orders are to be used in individual cases concerning, usually, particular subscribers. For example, on the basis of the provision of a particular name mentioned in the production order, a particular associated telephone number or e-mail address may be requested. On the basis of a particular telephone number or e-mail address, the name and address of the subscriber concerned may be ordered. The provision does not authorise Parties to issue a legal order to disclose indiscriminate amounts of the

service provider's subscriber information about groups of subscribers, like for example, for the purpose of data-mining [Explanatory Report, par. 170, 175, 182].

#### ***4.6 Search and seizure of stored computer data***

This article aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Domestic legislations include powers for search and seizure of tangible objects. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data, even if it *per se* will not be considered as a tangible object.

With respect to the search for evidence, in particular computer data, in the new technological environment, many of the characteristics of a traditional search remain, with the preconditions for obtaining legal authority to undertake a search remaining the same. However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. In the case of electronic data either the physical medium on which the intangible data is stored must be seized or taken away, or a copy of the data must be made in either tangible form, such as a computer printout, or in intangible form, such as a diskette, before the tangible or intangible medium containing the copy can be seized and taken away [Explanatory Report, par. 184, 186, 187].

#### ***4.7 Real-time collection of traffic data***

Article 20 addresses the subject of real-time collection and recording of traffic data for the purpose of specific criminal investigations or proceedings. Like real-time interception of content data, real-time collection of traffic data is only effective if undertaken without the knowledge of the persons being investigated. Thus, Internet Service Providers and their employees knowing about the interception must be under an obligation of secrecy in order for the procedure to be undertaken effectively. Paragraph 3 obligates Parties to adopt such legislative or other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any of the measures provided in this article concerning the real-time collection of traffic data. Paragraph 3 may be affected by the creation of explicit obligations in the law [Explanatory Report, par. 216, 225, 226].

#### ***4.8 Interception of content data***

Traditionally, the collection of content data in respect of telecommunications, for example, telephone conversations, has been a useful investigative tool to determine that the communication is of an illegal nature.

Given that computer technology is capable of transmitting vast quantities of data, including written text, visual images and sound and that the communication through the Internet tends to be the most popular way of communication, it has greater potential for committing crimes involving distribution of illegal content. "Content data" refers to the communication content of the communication, which is the meaning of the communication, or the message or information being conveyed by the communication [Explanatory Report, par. 228, 229].

### **5. Jurisdiction and international cooperation**

Article 21 establishes that Parties must enact laws so that they have jurisdiction of all the crimes described in the Convention if they occur in any of the four places the article mentions. In case more than one Party has jurisdiction over some or all of the participants in the crime, the affected Parties are to consult in order to determine the proper venue for prosecution where appropriate [Explanatory Report, par. 239]. Countries, however, are not bound to accept these possible ways to attain jurisdiction and, thus, countries like the United States, that seldom premises jurisdiction upon a nationality principle could easily ignore nationality as a base for acquiring jurisdiction [Viano C.E., 2004].

Chapter III (Articles 23- 35) contains a number of provisions relating to extradition and mutual legal assistance among the Parties. This was a significant point of the Treaty cybercrime legislation is plagued by a lack of geographically based jurisdictional boundaries. As Professor James Boyle noted, "If the king's writ reaches only as far as the king's sword, then much of the content on the Internet might be presumed to be free from the regulation of any particular sovereign", an observation which is particularly apt in the criminal enforcement context [Weber M.A., 2003].

Considering that it is impossible to regulate criminal behaviour without a means to ensure enforcement of sanctions, the objective of the drafters at this Chapter was to extend the ambit of the king's sword through cooperation.

Article 23 sets forth three general principles with respect to international co-operation. First, it declares that international co-operation is to be provided among Parties "to the widest extent possible". Second, it mentions that co-operation is to be extended to all criminal offences related to computer systems and data, as well

as to the collection of evidence in electronic form of a criminal offence, meaning that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system involves electronic evidence, the terms of Chapter III are applicable.

However, it should be noted that Article 24 (Extradition), according to which the obligation to extradite applies only to those crimes committed in Articles 2- 11, Article 33 (Mutual assistance regarding the real time collection of traffic data), according to which each Party is obliged to collect real time “traffic data” for another member country and Article 34 (Mutual assistance regarding the interception of content data), which discusses the cooperation and sharing of information obtained through means as eavesdropping and wiretapping, permit the Parties to provide for a different scope of application of these measures.

Third, it states that co-operation is to be carried out both “in accordance with the provisions of this Chapter” and “through application of relevant international agreements on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws”.

Article 25 requires mutual assistance “to the widest extend possible”, when Article 26, referring to those cases when a Party obtains important information that may assist another member country in a criminal investigation, calls them “spontaneous information”. Article 27 discusses mutual assistance in the case of absence of applicable international agreements. Article 28, which is applicable only when no mutual assistance treaty exists, provides for confidentiality and limitations on use of information, so as to preserve sensitive materials of a host country. Article 29 is the same as Article 16, except that it refers to international cooperation. Likewise, Article 30, is the mutual assistance version of Article 17. Article 31 requires that each member country have the ability to search, access, or seize “data stored by means of a computer system located within its territory” for the benefit of another member country. Article 32 merely makes it permissible for a source of data that already is publicly available to be available to a Party unilaterally and without a mutual assistance request, while at the same time, not preparing a comprehensive, legally binding system. Parties become, through Article 35, members of a 24/7 network, in order to face effectively crimes which require a rapid response.

Improving a state’s legal ability to provide and receive international cooperation to face cybercrime effectively is not merely a question of improving its laws related to mutual assistance and extradition, but, there is a significant relationship between the legal ability to provide international cooperation and the quality of a state’s laws that define crime, establish legal investigative powers and provide

safeguards. In order for the states to achieve the above goal, a number of measures [Piragoff K.D., 2004] have been proposed.

## 6. Additional Protocol

The first Additional Protocol on Racism and Xenophobia on the internet (ETS 189) has been opened for signature in Strasbourg, January 26, 2003.

The Convention, as the most recent international instrument in its field, binds its ratifying Parties, shapes their domestic laws but also, functions as a model law for those Parties that consider to accede, or serve as a model law for other states. In particular, the substantive part is meant as a framework, where new and other IT-related misuse will be added to the Convention in the form of additional protocols, like this first one, so that the Convention gives its full effect, when these protocols come into force [Kaspersen W.K.H., 2004].

The Additional Protocol after defining “racist and xenophobic material” as “any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors”, proposes, with its Articles 3-6 certain measures to be taken at national level so as to criminalize acts of a racist and xenophobic nature committed through computer systems. Article 7 criminalizes aiding and abetting the commission of any of the offences established in accordance with the Protocol, with intent that such offence be committed. Article 8, paragraph 1 states that Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, *mutatis mutandis*, to this Protocol and paragraph 2 states that the Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol. Final provisions are included in articles 9-16.

## 7. Opposition to the Convention

The Convention on cybercrime, as any pioneering legal tool, faced severe criticism and opposition.

Among the arguments against the Convention is the claim that the Treaty restricts freedom of expression online.

Another argument against the Convention is that it overstrains the investigative powers of police forces and governmental organizations, meaning that the government is granted an excessive amount of investigatory power, which is best illustrated in the example of call data vs. “traffic data”.

Before the Treaty, law enforcement agencies were allowed to seek call related data, such as the phone numbers that are dialed and the duration of the calls. However, under the Convention, law enforcement authorities would have the right to wide-ranging "traffic data," which includes the source, destination, and duration of calls, as well as the type of traffic or the sort of services consulted. A point of discussion is whether it is a violation of privacy if an Internet Service Provider is forced to inform law enforcement agencies about the downloads, e-mails and duration of visits to particular websites a client did [Keyser M., 2003]. The American Civil Liberties Union claims that U.S. authorities will use the Convention to conduct surveillance and searches that would not be permitted under current U.S. law. European critics worry that the Convention allows the transfer of personal data to countries outside Europe—such as the United States—that they believe have less protective laws regarding the use of such information. Council of Europe officials dismiss such fears, arguing that the Convention provides adequate civil liberty safeguards and limits information transfers to specific criminal investigations [Archick K., 2002].

Another point of criticism is that the Treaty obliges companies and individuals to provide law enforcement with far greater information than is considered the norm under most telecommunications laws. ISPs and other related businesses keep "subscriber data", which is confidential client records and they are unwilling to offer them to an investigating governmental agency. Moreover, companies are concerned with the increased costs associated with retaining and preserving data should an order be served upon the company to do so and it is ultimately the consumer that will need to weigh the importance this cost [Keyser M., 2003]. Meanwhile, some business and consumer groups are concerned that the Convention's provisions that increase costs to service providers, impede the development of security technologies and sale of encryption programs, and negatively affect consumer confidence in e-commerce.

Another hot topic is that the Convention infringes upon citizen civil liberties. Article 15 requires member countries "to establish conditions and safeguards to be applied to the" governmental powers established in Articles 16 thru 21. Those conditions and safeguards are required "to protect human rights and liberties". Article 15 in fact "lists some specific safeguards, such as requiring judicial supervision, that should be applied where appropriate in light of the power or procedure concerned" [Keyser M., 2003].

The Global Internet Liberty Campaign (GILC), a non profit, non governmental organization, whose member organizations have joined together to protect and promote fundamental human rights such as freedom of speech and the right of privacy on the net for users all over the world, is strongly opposed to certain



guidelines of the Treaty. GILC has drafted two letters against the Treaty's provisions because it believes that they run contrary to internationally accepted human rights norms and infringe on the free speech and privacy rights of all internet users [GILC, 2000].

On the other hand, some analysts criticize the Convention as being too "indulgent" or "soft", because of not permitting police authorities direct crossborder access to computer data, which they argue creates an extra, time-wasting step [Archick K., 2002].

Another point of consideration is that the states that participated in the Convention's negotiations are not the "problem countries" in which cyber criminals operate relatively freely. Hackers frequently route cyber attacks through portals in Yemen or North Korea, neither of which are part of the Convention, so sceptics point out that for the Convention, in order to serve as a deterrent, more states will have to sign it and abide by its mandates. As an example, it is noted that the Filipino author of the "I Love You" virus that caused millions of dollars in damage worldwide in 2000 was never prosecuted because no applicable laws existed [Archick K., 2002].

## 8. Conclusion

Computer crime, and especially cybercrime, is not a specific new form of crime, but rather a wide variety of new phenomena, which encompasses both new types of crimes, as well as traditional crimes committed in connection with computer systems or computer networks [Sieber U., 2004]. This represents a tremendous challenge for the criminal law.

The Convention on cybercrime is based on three pylons. First, it defines criminal offenses and sanctions under their domestic laws for four categories of computer-related crimes—fraud and forgery, child pornography, copyright infringements, and security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability. Second, it establishes domestic procedures for detecting, investigating, and prosecuting computer crimes, and collecting electronic evidence of any criminal offense. Such procedures include the expedited preservation of computer-stored data and electronic communications, search and seizure of system, and real-time interception of data. Third, it establishes a rapid and effective system for international cooperation. The Convention deems cybercrimes to be extraditable offenses, and permits law enforcement authorities in one country to collect computer-based evidence for those in another. It establishes a 24/7 contact network to provide immediate assistance with cross-border investigations.

Above all, parties to the Convention must guarantee the conditions and safeguards necessary to protect human rights and the principle of proportionality.

There is no doubt that the Treaty represents a flexible and effective vehicle in combating cybercrime and a useful tool in harmonizing the law and improving cooperation between legal systems in the field of computer crime. The fast changing nature of cybercrime, nevertheless, necessitates both the monitoring of future developments in computer crime and further analysis of new threats which the criminal law will be required to address [Sieber U., 2004]. Moreover, the sensitive nature of the fundamental human rights, such as the privacy and freedom of speech, require borders at the guidelines and the procedures which restrict them.

## References

[Aldesco I.A., 2002]	Aldesco I.A. (2002), The demise of anonymity: A constitutional challenge to the convention on cybercrime, Loyola of Los Angeles Entertainment Law Review, 81
[Hopkins L.S., 2003]	Hopkins L.S. (2003), Cybercrime Convention: A positive beginning to a long road ahead, Journal of High Technology Law, 101
[Marshall J.J., 2005]	Marshall J.J. (2005), The Convention on cybercrime: A harmonized implementation of international penal law: what prospects for procedural law process?, Comp. & Info. Law, 329
[Council of Europe]	Council of Europe, Treaty Office, online at <a href="http://conventions.coe.int/Treaty/EN/v3Glossary.asp">http://conventions.coe.int/Treaty/EN/v3Glossary.asp</a> /accessed 11.10.2003
[Brierly J.L., 1963]	Brierly J.L. (1963), The law of Nations: An introduction to the international law of piece 57, Humphrey Waldock ed., Oxford Univ. Press 6th ed.
[Preamble, par.4]	Convention on Cybercrime, Preamble, online at <a href="http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm">http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm</a> /accessed 03.04.2011
[Explanatory Report, par.##].	Convention on Cybercrime, Explanatory Report, online at <a href="http://conventions.coe.int/Treaty/en/Reports/Html/185.htm">http://conventions.coe.int/Treaty/en/Reports/Html/185.htm</a> /accessed 03.04.2011
[Viano C.E., 2004]	Viano C.E. (2004), Computer crimes and criminal law: international dilemmas and approaches, Round Table II of the 17th International Congress of Penal Law, Ant.N.Sakkoulas, 51-52, 67
[Weber M.A., 2003]	Weber M.A. (2003), Berkeley Technology Law Journal, 425

[Piragoff K.D., 2004]	Piragoff K.D. (2004), International cooperation in combating cyber-crime and cyber-terrorism, Round Table II of the 17th International Congress of Penal Law, Ant.N.Sakkoulas, 192-193
[Kaspersen W.K.H., 2004]	Kaspersen W.K.H. (2004), Gathering electronic evidence, Round Table II of the 17th International Congress of Penal Law, Ant.N.Sakkoulas, 80-81
[Archick K., 2002]	Archick K. (2002), CRS Report for Congress, Cybercrime: The Council of Europe Convention, online at <a href="http://www.usembassy.it/pdf/other/RS21208.pdf">http://www.usembassy.it/pdf/other/RS21208.pdf</a> /accessed 10.04.2011
[Keyser M., 2003]	Keyser M. (2003), Transnational Law and Policy Journal, Vol. 12. 12:2, 324-326
[GILC, 2000]	GILC (2000), The letters drafted by GILC are available online at <a href="http://gilc.org/privacy/coe-letter-1000.html">http://gilc.org/privacy/coe-letter-1000.html</a> and <a href="http://gilc.org/privacy/coe-letter-1200.html">http://gilc.org/privacy/coe-letter-1200.html</a> / accessed 15.03.2011
[Sieber U., 2004]	Sieber U. (2004), Computer crimes, cyber-terrorism, child pornography and financial crimes, Round Table II of the 17th International Congress of Penal Law, Ant.N.Sakkoulas, 47-50

### **Appendix: Council of Europe Convention on Cybercrime**

Chart of signatures and ratifications, ETS no 185.

Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States.

Online at

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185-&CM=&DF=&CL=ENG>/accessed 26.04.2011

Status as of 01.04.2011

Opening for signature

Place: Budapest

Date: 23.11.2001

Entry into force

Conditions: 5 Ratifications

including at least 3 member States  
of the Council of Europe

Date: 01.07.2004

## Member States of the Council of Europe

States	Signature	Ratification	Entry into force
Albania	23/11/2001	20/6/2002	1/7/2004
Andorra			
Armenia	23/11/2001	12/10/2006	1/2/2007
Austria	23/11/2001		
Azerbaijan	30/6/2008	15/3/2010	1/7/2010
Belgium	23/11/2001		
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006
Bulgaria	23/11/2001	7/4/2005	1/8/2005
Croatia	23/11/2001	17/10/2002	1/7/2004
Cyprus	23/11/2001	19/1/2005	1/5/2005
Czech Republic	9/2/2005		
Denmark	22/4/2003	21/6/2005	1/10/2005
Estonia	23/11/2001	12/5/2003	1/7/2004
Finland	23/11/2001	24/5/2007	1/9/2007
France	23/11/2001	10/1/2006	1/5/2006
Georgia	1/4/2008		
Germany	23/11/2001	9/3/2009	1/7/2009
Greece	23/11/2001		
Hungary	23/11/2001	4/12/2003	1/7/2004
Iceland	30/11/2001	29/1/2007	1/5/2007
Ireland	28/2/2002		
Italy	23/11/2001	5/6/2008	1/10/2008
Latvia	5/5/2004	14/2/2007	1/6/2007
Liechtenstein	17/11/2008		
Lithuania	23/6/2003	18/3/2004	1/7/2004
Malta	17/1/2002		
Moldova	23/11/2001	12/5/2009	1/9/2009
Monaco			
Montenegro	7/4/2005	3/3/2010	1/7/2010
Netherlands	23/11/2001	16/11/2006	1/3/2007

Norway	23/11/2001	30/6/2006	1/10/2006
Poland	23/11/2001		
Portugal	23/11/2001	24/3/2010	1/7/2010
Romania	23/11/2001	12/5/2004	1/9/2004
Russia			
San Marino			
Serbia	7/4/2005	14/4/2009	1/8/2009
Slovakia	4/2/2005	8/1/2008	1/5/2008
Slovenia	24/7/2002	8/9/2004	1/1/2005
Spain	23/11/2001	3/6/2010	1/10/2010
Sweden	23/11/2001		
Switzerland	23/11/2001		
The former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005
Turkey	10/11/2010		
Ukraine	23/11/2001	10/3/2006	1/7/2006
United Kingdom	23/11/2001		

#### Nom-member States of the Council of Europe

States	Signature	Ratification	Entry into force
Argentina			
Australia			
Canada	23/11/2001		
Chile			
Costa Rica			
Dominican Republic			
Japan	23/11/2001		
Mexico			
Philippines			
South Africa	23/11/2001		
United States of America	23/11/2001	29/9/2006	1/1/2007

Total number of signatures not followed by ratifications: 17

Total number of ratifications/ accessions: 30

# **Ethical implications concerning the access to and use of information and the technologies**

---

---

**Antonio Cobos Flores**

---

---

## **1. Introduction**

Nowadays, much is commented on the importance of access to and use of information. Information is considered one of the assets that provide users – considering everyone is an information user – with the most added value, and it is even quoted that it is one of the main goods of the developed countries as compared to the developing countries, in which mostly production of the primary sector of economy takes place: agricultural products and raw materials in general.

The age we live in is characterized by a series of changes in the way information is generated, distributed and obtained. We are witnesses of the transformation from printed to electronic media. The use of the Internet as an alternative to produce, broadcast and obtain information is becoming more common every day.

For a few decades now, “information” has been turning into a topic, as ubiquitous as imprecise, that seems to respond to the economical demands of a globalized society. It is used to satisfy specific needs that emerge in a person or a society.

Its use must follow certain lineaments that give credit to the authors of the available resources. This leads us to ethics. Today, ethics are an obliged reference about principles that should guide our actions. Even if the importance of theoretical discussion is accepted, it is necessary to visualize and understand the practical effects and implications that the admittance of ethical values at every level of our society comprehends.

But the very access to electronic information implies that any person can infringe copyright, moral or patrimonial.

## **2. Information and the technological development**

overall, technology has modified many of the social activities and relationships in recent years; particularly, computing and telecommunications have become remarkably popular. It is worth mentioning that the meaning of the word “technology” is understood as the compound of knowledge relating to the skills humanity has to produce and build goods; that is, the industrial arts at the disposal of a so-

ciety. Technology is the most important source of change known to mankind. Its transforming force might overwhelm us if we do not know how to use it for our own benefit, something we could avoid if, instead of taking a resisting position, we decide to use it on our behalf.

The introduction of technology to the field of information storage and recovery, known as information technologies, has motivated innovative ways of organizing work. Its use, apart from inducing a new division to produce, distribute and save information and knowledge, has sprung a new criteria to determine their exchange value and has generated social processes in order to organize it and keep it. This generates a new paradigm of documental organization different in nature to the one created by the culture of printed media since the Enlightenment back in the 18th century.

In this sense, we might consider Estela Morales's words: "Technology has been one of the areas that have shown more development, constant change and innovation this century. And information – its origin, representation, distribution and recovery – has been affected and benefited by its progress, to the degree that a section with own personality exists worldwide and it is known, precisely, as information technologies." (Morales, 2003, p.33)

The use of these technologies is provoking the globalization of information. On its way to this globalization, the Internet plays a major role due to the immense possibilities with which it provides an ordinary user, receiver of information, turning him into a sender and administrator of his own information on the Web.

"Through the years, a person's need of information was satisfied when visiting a library, by means of the orientation or reference of documental materials from the librarian. If literature already surpassed the individual then, the arrival of information and communication technologies caused a substantial change in our society, mainly in the way information is created, manipulated and distributed, to the extent that the ICTs are present in every productive process of the society we live in." (Hernández, 2009, p. 1)

The Internet represents the most significant change concerning the creation and distribution of information, since it is a colossal web capable of storing and favoring the interchange of information nearly limitlessly. Mankind had never seen such a system capable of offering such a degree of interactivity before.

A few characteristics of the access to information via the Internet are:

- Easy access to all kinds of information, on any topic and in any format. Information is the raw material we need to create the knowledge with which we face the problems that arise everyday at work, at home, or while reflecting.

- Channels of immediate, synchronous and asynchronous communication, to spread information and contact any person or institution in the world by means of the edition and diffusion of information in web format, e-mail, instant messaging services, telematic forums, video conferences, blogs, and the wikis.
- Task automatization, by programming the activities we want computers to execute; these constitute the backbone of all ICTs. This is one of the essential characteristics of computers, which definitely are “machines that process information automatically, following instructions from programs.”
- Interactivity. Computers allow us to interact with document management systems, videogames, multimedia educational materials and specific expert systems. This interaction is the consequence of the fact that computers are programmable machines and it is possible to define their function determining the answers they should provide as a response to the users’ different actions.
- Cognitive instrument that foster our mental abilities and allow the development of new ways of thinking.

During the first years of the 1990s, the emergence of one of the most popular Internet services, the www, favored the birth of a new battlefield, this time a virtual one. Big companies began competing for an adequate position among both the mass of cybernauts and the most important web search engines. The presence of the Internet started becoming indispensable in the business world.

Besides that, it could be said that a person’s use of information depends on that individual’s current task; this is to say, information can be used to fulfill certain activity. In many cases such activity is academic, so information is basically used to satisfy learning needs. Nonetheless, the user’s autodidacticism that exists on many occasions should not be diminished; it is expected that information will be eventually useful for that person. According to Patricia Hernández (Hernández, 1997, p. 3), the motivation to search, recover and use information has an eminently utilitarian nature related to production. Even to the researchers who seemingly use information without practical, immediate purposes, this use is based on the necessity of producing knowledge, or simply support decision making.

“People diversely aged, with different education levels and belonging to different social, political, and ethnical groups have access to information. They use it consciously or unconsciously, that is, they reach it because of necessity, interest, or curiosity through game programs and hypermedia; from that point, they might even become addicted to that technology. This is the case of, above all, the new generations who are also users of information and libraries, and very often are more familiar with audiovisual and electronic media than with the one printed



on paper." (Morales, en línea <<http://ifla.queenslibrary.org/IV/ifla61/61-more.htm>>)

There is no doubt about the fact that the way we work, study, amuse ourselves, relate to each other, and use information is being modified by technology ever since the appearance of computers. It is for that reason that the concept of ethics in relation to the use of information is traced back to the 1970s, when computers were first used massively for scientific and technical applications. Then, questionings about the storage and accessibility of documents included in bibliographical data bases sprang. Later, the concept was extended by the massive use of the Internet and the abuses of this technology.

Technologies propose new lifestyles and ways of thinking; they bring up new paradigms of relationships between individuals, the cause of ethical problems regarding the use of technologies and the need of research for solutions to achieve social wellbeing and to preserve an informatics culture in the organizations. The fast evolution of the information and communication technologies is perturbing, directly and indirectly, the moral values, and this entails the misuse information is given, thus provoking ethical dilemmas and threats to the behavior and conduct of the individuals, the society and the organizations.

The concern about understanding actions parting from ethical principles has been present for the most relevant philosophers. For example, Aristotle represents the culmination of an entire philosophical school for which ethics should determine the aim of our interests; this is what would make a man virtuous and wise, what would permit the true pleasure given to happy men. It is all about living morally in order to choose the practice of justice. In justice, men achieve the main ethical virtue and right, society and citizenship are based on it. Individuals should be endowed with basic and fundamental moral principles, universal obligations that make an optimal and fair social development possible for them.

Respecting the authorship of those who generate information is a universal obligation, named information ethics. Information ethics deal with all what is related to the proper and wrong uses of information; they consider aspects such as intellectual property, access to free or restricted information, censorship, use of information from public institutions, confidentiality and integrity of data, and the international flux of information, among others.

Apart from that, it could be said that it is not sufficient to acquire and organize information; it is necessary to keep it available when needed too. From the technological point of view, it is essential to provide all users with every chance of accessing information. However, gaining access is not that simple, for political and economical restrictions, normative deficiencies, and limitations imposed

by powerful groups, such as censorship, manipulation and corruption present at every stage of the process, should not be ignored.

Also, information might be enriched or distorted due to the interpretation of the person who is selecting, analyzing, or summarizing it, who labels it and searches for it in a catalog or database, either because of the technical nature of their work or because it is convenient for a political system, economical group, or simply marketing factors.

Changes in the context of computing activity demand modifications to the ways work is dealt with and, subsequently, to the information user's ethics. These changes do not consist of variations in the moral essence but instead of the introduction of new ethical conducts that are necessary for a renewed environment. According to the Special Libraries Association (available at <http://www.sla.org>), nowadays information professionals require:

- Sense of commitment to service excellence.
- Capabilities to deal with and look for the challenge, as well as to identify new opportunities inside and outside the library.
- A wide perspective.
- A gift for searching links and associations.
- Skill to create respectful and friendly environments.
- Communication skills.
- Ability for team work.
- Leading spirit.
- To know how to plan, prioritize and approach critical aspects.
- To be committed to a continuous formation and development of their professional career.
- A gift for business and for identifying new opportunities.
- To recognize the value of cooperation and solidarity among professionals.
- To be flexible and to have a positive attitude towards constant change.

### **3. Ethics, technology, access and use of information**

in the middle of the age of information, the possibilities of the Internet as massive communication media have motivated many authors to use the web for promoting, publishing and distributing their works. After a single click, any user can have access to these intellectual works from home in a matter of seconds.

It is because of that that the production and reception of information should be articulated according to certain criterion relevance, such as: (Leme, 2001)

- Reach: Who would potentially be interested in knowing the information?
- Density: At what level information is articulated with the web of social knowledge and practices?
- Purpose: What effects could it cause? What consequences would it have on the web of knowledge?
- Impact: What would be the possible deployments at the historical moment in which it is produced or spread?
- Originality: To what extent is the information unknown to the audience who can have access to it or at whom it is aimed?
- Reliability: To what extent the information can be verified or confirmed?

This criterion should not be considered as permanent principles inherent to information, but as coming from the ethical, political and economical implications of its production and distribution. This means their pertinence depends on the analysis of the social milieu to which they are applied (scientific, artistic, journalistic, pedagogical, political, etcetera) and the circulation environment (public places, universities, social organizations, churches, etcetera).

The availability of the technology to access to and use information might bring up a great number of possibilities of use and abuse. It is not always possible to anticipate those cases in which ethics will be under scrutiny and many of these matters are analyzed generally once they have happened.

It is undeniable that the availability of technology tends to be associated with social groups with a greater economical power, and this provokes that, while such groups make an exhaustive use of technologies and dispose of more knowledge about them, groups with lesser resources tend to have limited knowledge and power on such technologies.

Likewise, information technologies change the lifestyles, habits and customs, thus allowing something that was unfeasible or unlikely before them. So it is worth questioning about the changes information technologies generate in the ethical values.

Laudon (2004, <<http://ellibrolibre.com.ar/descargas/laudon.pdf>>) proposes five moral dimensions to assess the age of information:

1. Rights and responsibilities: What are the individuals and corporations' rights regarding information and themselves? What are the legal means to protect that information? What are the responsibilities related to it?
2. Property rights: How are the classic concepts of patent and intellectual property moved into digital technology? What are those rights and how are they protected?

3. Responsibility and control: Who is responsible of controlling the use and abuse of people's information?
4. Systems quality: What data standards, information and processing programs must be required to guarantee the protection of individual and social rights?
5. Life quality: What values must be preserved and protected in a society based on information and knowledge? What institutions should protect them and which should be protected?

These five dimensions represent a good guideline on the considerations, questions and ethical answers that a person should make when accessing, recovering and using information in technological mediums.

The Internet provides us with a third world in which we can do almost everything we do in the real world; additionally, it allows us to carry out new activities, many of which are enriching for our personality and way of life (contact with telematics and people from around the world, instant localization of any sort of information, telecommuting, teleformation, teleleisure, among others). Now, people can distribute their time interacting in three worlds: present world, of physical nature, constituted by atoms, ruled by the laws of space, in which there are distances between people and things; the intrapersonal world of imagination; and the cyberspace, of virtual nature, made from bits, without any distances. It is to move throughout this third world that we must review and/or generate ethics.

It should be considered, once more, that technologies constantly change and things that used to be impossible or excessively costly, all of a sudden become accessible assets – first, for a more powerful minority, then, for the masses – with which come increased risks of legal and ethical violations yet again.

It is worth saying that it concerns each society to analyze and respond to these new dilemmas and to fix new moral rules according to their ethical principles, their own customs, their culture, and their moral system. There will be more prepared societies, those which demand technology, and less prepared too, the ones that adopt technologies. Nevertheless, it is undeniable that both will have to respond to these new ethical dilemmas. For that reason, it is so necessary to implement rules and regulations so free access to information during the age of information and communication technologies can find an equilibrium related to the correct use that information must be given.

#### 4. Conclusions

Today we live in what has been dubbed the third technological revolution. One of its main foundations is the development of the new information and communication technologies, characterized by the integration of informatics, telecommunications and webs for electronic data interchange.

Technological development has caused such an impact on nowadays world essentially because of a phenomenon that goes beyond the amazement of technology; that is, the inexhaustible need for access to an essential raw material: information.

In the globalization process going on these days, information acquires key importance in ordering the various social structures.

It is not possible to make a universal discourse about technologies, since the problems that spring today regarding the access to information and the new information and communication technologies are not mainly scientific or technological. In science, we have knowledge; in technology, the tools. Problems are basically political, economical, social and cultural.

Neither a purely triumphalist attitude is applicable in relation to the wonder of technological progress. History shows us that the problem lies in the use everyone makes of technology. It is evident that not every goal we have assigned to it has dignified our existence. This is something that happens nowadays and, for obvious reasons, it will keep on being the pattern of human behavior, particularly because we exert our freedom in every act, this is no exception. In such sense, these words serve as a conclusion regarding the ethical questions in the field of technological development.

Ethics concerning the use of information in all social contexts are being seriously assessed. Moreover, in the process of globalization occurring these days, information acquires a key role in ordering the different social structures. We should remember a widely recognized question: the least the information, the more disadvantages in terms of development.

#### *Works consulted*

Cobos Flores A. (2009). La industria editorial en México frente a las tecnologías de la información y comunicación. - México: el autor (Tesis Licenciatura en Bibliotecología y Estudios de la Información): UNAM, Facultad de Filosofía y Letras, 89 p.

Cobos Flores A. (2009). El papel de la biblioteca en torno a la sociedad del conocimiento. En: Revista biblioteca universitaria, vol. 12, no. 2, julio-diciembre, pp. 132-139.

García Pérez, J.F. (2004). Los derechos de autor, en entorno digital y los usuarios. – México: El autor (Tesis Maestría en Bibliotecología y Estudios de la Información): UNAM, Facultad de Filosofía y Letras, 272 p.

Hernández Pérez, J. (2009). Análisis de las interacciones de google como motor de búsqueda y la bibliotecología. – México: el autor (Tesis Licenciatura en Bibliotecología y Estudios de la Información): UNAM, Facultad de Filosofía y Letras, 101 p.

Hernández Salazar, P. (1997). Seminario Latinoamericano sobre formación de usuarios de la Información y los estudios de usuarios. - México: UNAM, Centro Universitario de Investigaciones Bibliotecológicas. p. 3.

Leme Brito, L. P. (2001) “Información y participación social”. En: I Coloquio Latinoamericano y del Caribe de servicios de información a la comunidad.

Laudon Kenneth C. (2004). Sistemas de información gerencial [en línea] <<http://ellibrolibre.com.ar/descargas/laudon.pdf> > [Consultado: 30 de diciembre de 2010]

Márquez Fernández, A. (2001). “La ética del investigador frente a la producción y difusión del conocimiento científico” En: Revista Venezolana de Gerencia, Vol. 6, No. 16, octubre-diciembre, pp. 632-650.

Morales Campos, E. (2001). La diversidad informativa latinoamericana en México/Estela Morales Campos. – México: UNAM, Centro Coordinador y Difusor de Estudios Latinoamericanos, 386 p.

Morales Campos, E. (2003). Infodiversidad, globalización y derecho a la información. Buenos Aires: Sociedad de Investigaciones Bibliotecológicas, 203 p.

Morales Campos, E. (2006). Infodiversidad y cibercultura: globalización e información en América Latina. - Buenos Aires: Alfagrama, 172 p.

Morales Campos, E. Los medios alternativos a la industria editorial para obtener información [en línea] <<http://ifla.queenslibrary.org/IV/ifla61/61-more.htm>>

Seminario Latinoamericano sobre formación de usuarios de la Información y los estudios de usuarios / Patricia Hernández Salazar, coord. - México: UNAM, Centro Universitario de Investigaciones Bibliotecológicas, 85 p.

Villalobos G. F. (2004). “Implicaciones éticas y socioculturales del uso de las tecnologías de la información y la comunicación”. En: Revista venezolana de ciencias sociales, vol. 8, No. 1, enero-junio

# **Online copyright infringement provisions within UK's Digital Economy Act, 2010 - Are Internet Service Providers legally responsible for their subscribers?**

---

---

**Eben Duah**

---

---

## **Introduction**

Since the launch of the peer-to-peer (P2P) programmes in the late 1990s, file-sharing has featured prominently in online copyright infringement debates. There have been strategies to try to reduce such unlawful activities which have encompassed legal actions against P2P vendors and individual infringers, while internet service providers' (ISPs) have also been requested to comply with procedures such as notice and take-down and install filtering systems. Although, the legal actions have resulted in shutting down most of the mainstream P2P networks including *Napster* (2001) and *Grokster* (2005), and court requests seeking to get users' identities from ISPs have largely been granted through disclosure orders, (or Norwich Pharmacal orders) there are still problems with these strategies. For example, the decentralised architecture of the P2P networks has made it difficult for right holders to pinpoint where to level blame, individuals have increasingly been resorting to the use of pseudonyms or virtual private networks to evade or complicate detection, and particularly the cost ineffectiveness of legally pursuing the millions of illegal file-sharers with the low risk of prosecution appears to have led to a rethink and thoughts of a new focus.

## **ISPs in the picture**

In an effort to find an alternative solution, there have been calls for ISPs to take a more active role in 'policing' their networks by being part of a technical enforcement regime, popularly referred to as the "graduated response" or "three strikes" approach. The graduated response model (GRM) proposes to begin with the gathering of evidence through the harvesting of alleged infringers' internet protocol (IP) addresses. It also involves the notification of alleged infringement and internet traffic management which the International Federation for the Phonographic Industry (IFPI), in particular has been demanding governments to require ISPs to enter into cooperative relationship with right holders in order to fight illegal file-sharing. Global reception to this model have been, and as to be expected, mixed. Although, some countries such as South Korea and Taiwan have already incorpo-

rated the GRM into their domestic copyright enforcement systems (De Beer and Clemmer, 2009) and the United States (Anderson, 2008) and Ireland (Anderson, 2009a) have agreed to voluntary schemes, Germany and Finland have so far refrained from, or rejected the GRM implementation, - just to name but a few. (Cheng, 2009; Llewellyn, 2009; Moya, 2010) Within Europe, there have been two major developments regarding GRM legislation. France adopted a so-called HADOPI law in 2009, (HADOPI in English: "Higher Authority for the Diffusion of Works and the Protection of Copyright on the Internet") while the UK's Digital Economy Act (DEA) passed into law in 2010 also has provisions to essentially impose a GRM obligation on ISPs. Before discussing the DEA provisions and the ISP obligations which form the core of this paper, it is vital to provide a brief background to the HADOPI law which appears to be a pioneered GRM legislation.

### The French HADOPI

In 2006, the French adopted the DADVSI law, (*in English: "law on authors' rights and related rights in the information society"*) which implemented Directive 2001/29/EC. The DADVSI had provisions (Article L.335-12 of the Intellectual Property Code) that obliged subscribers to monitor their accounts to ensure that no file-sharing occurred. The DADVSI however faced challenges including the practicalities of prohibiting all P2P transferring activities, while it was also believed to restrict the right to copying copyrighted works for private use due to its text on the digital rights management. The French Constitutional Counsel then struck down several of its major provisions based on its unconstitutionality, (Decision no. 2006-540 DC, 27 July 2006) thereby making the DADVSI much weaker in terms of fighting online copyright infringement.

However, that did not frustrate the French pursuit for online copyright infringement legislation and France eventually became the first EU Member State to put into effect GRM legislation as a way of enforcing copyright on the internet by sanctioning users. It began with the construction of the *HADOPI-1* (Bill), described as more suitable and efficient measure than the DADVSI provisions to fight illegal file-sharing (May and Liens, 2009). The key goals of this bill were the setting up of an administrative authority called HADOPI, to oversee the implementation of a GRM regime which would include the suspension of internet access alongside the education and promotion of legal online alternatives without the involvement of any judicial authority. Nonetheless, the French Constitutional court called for amendment to parts of the bill, (Decision no. 2009-580 DC, 10 June 2009) citing some of the texts as in breach of an individual's freedom of expression under the Constitution. The Counsel, utilising its powers under Article 61(2) of the French Constitution (1958), also observed illegitimacy on the judicial role of the administrative authority with no recourse to the courts.



Besides, there were concerns as to whether due-processes had been adhered to, in areas such as fair trial, the presumption of innocence and the right to defence, (Lucchi, 2011). These concerns were to be addressed with a revised *HADOPI-2* to overcome constitutional challenges, so as to pave the way for the enactment of the so-called *HADOPI* law in 2009. It must be pointed out that the adoption of *HADOPI-2* has also been challenged, but rather unsuccessfully, as opponents still believe it raises, amongst other things, issues of privacy to which internet subscribers are entitled. With the *HADOPI* law now passed, its implementation process involves detection by the copyright owners of potential infringements (based on IP addresses) over P2P networks to be reported to the *HADOPI* administrative authority. The *HADOPI* authority then consults with other parties involved, and if contented, contact the relevant ISPs to seek the identification of these alleged infringers (May and Liens, 2009), while also requiring the ISP to send the first notification to the matched subscriber (Lovejoy, 2011). A second notice is sent, if the IP address of the subscriber first notified is suspected of being engaged in another infringement over the subsequent six months (Lovejoy, 2011). If within one year after the second notice, a user's IP address again appears among those reported to the *HADOPI* authority, the user will then be subjected to judicial procedures to determine guilt, where penalties ranging from fines through to the disconnection of an internet could be expected, but with the option of subscribers appealing the judge's decision, (Stroussi, 2009). Some commentators argue that this procedure is disproportionate on the basis that a referral of repeat offenders to a judge may result in nothing more than the judge overseeing a penalty being imposed without oral hearing from the alleged infringer in defence of the allegation. With minimal participation of the parties to determine guilt, it gives the impression of a set-up akin to an administrative body with a legal representative just "presiding over" decisions, (Stroussi, 2009). Does this procedure not challenge the 'presumption of innocence' principle? (Article 9 of the Declaration of the Rights of Man and of the Citizen of 1789).

Other concerns also point towards whether or not subscribers' access to other IP based services would be unaffected in the event of an internet suspension. According to Horten, (2009) there may be the difficulties in applying internet suspension across France without affecting some account holders' other subscriptions within a package (Horten, 2009). Horten's findings appear to be based on a reference to an assessment by the French regulator (ARCEP) which indicates that in areas where there is no local loop unbundling, it will be impossible to maintain IP-based voice services, when terminating internet access. If this occurs, the "disproportionate" arguments will be strengthened. However, despite the criticisms, doubts of unconstitutionality and unprecedented debates surrounding *HADOPI-2*, its implementation by the French government has seen suspected

copyright infringers receiving warning letters since September, 2010 (Forde, 2010) Let us now focus on the UK legislation, the Digital Economy Act 2010.

### **The Digital Economy Act (DEA)**

The UK became the next European Union (EU) Member State, after France, to legislate on the GRM by passing the DEA in 2010. The enactment of the DEA has been the culmination of proposals and consultations following recommendations from the Gowers Report in 2006 and then the Digital Britain report (DBR) in 2009 when the digital inclusion targets were set and the objective of reducing illegal file-sharing by encouraging cooperation between ISPs and rights holders was outlined (Carter, 2009). This was followed by the Digital Economy Bill in the same year which adopted a number of proposals set out in the DBR. With the passing of the DEA, the United Kingdom's (UK) communications regulator (OFCOM) has been responsible for the specification, procedural and enforcement elements of the obligations through the approval or adoption of legal binding codes of practices. Before the examination of the contested DEA provisions, a background to the status and origin of the obligations code are set out below.

#### ***Initial obligations***

Driven in part by the fact that existing strategies are not working, the DEA 2010, through its amendment to the Communications Act 2003 (CA 2003), imposes specific initial obligations on the ISPs, within sections 124A CA 2003 and 124B CA 2003, with the prescribed content of the initial obligations in 124E CA 2003. A GRM within the DEA commences with the supply of a copyright infringement report (CIR) by the rights holder to the appropriate ISPs (usually within a month of the alleged detection of the infringement) including details of the subscriber's internet protocol (IP) address and evidence of the infringement and the time of occurrence. The ISP is then required, also within one month of the receipt of the CIR, (and pursuant to 124A (4)), to notify the subscriber of the alleged offence, (as set out within 124A (6)) while also designing and maintaining a copyright infringement list (CIL). ISPs must also suggest alternative legal channels for copyrighted material consumption and convey any other advice, deemed helpful to the alleged infringer, (124A (8)) Section 124B CA 2003 then imposes upon ISPs an obligation to provide copyright infringement list (CIL) in a non-identifying format to copyright owners upon request, or as the initial obligations code requires the ISPs to comply, for rights holders to be able to secure a court order to then learn of the identity of the serial offender for possible legal action. The initial confusion from this information exchange may raise the question why the copyright owners would somehow be able to write a CIR for the ISPs then require

a set list from the ISPs based on the CIRs. The clearest assumptions may be that, the copyright owners have no way of identifying any alleged infringer, simply by the IP addresses alone and since ISPs would normally not disclose the identity without a court order due to the confidentiality agreements they have with their subscribers, the information that passes 'to-and-fro' (as the code may dictate) eventually enables right holders to obtain a disclosure order. Furthermore, some of the subscribers are assigned new (dynamic) IP addresses each time they are connected to the internet, hence, the information provided in the CIL will ensure a match of any particular infringement with the specific account holder.

### ***Technical obligations***

While there was the initial fear of an imminent termination of subscriber's internet access after the warnings, such as within the HADOPI law, there is no such imminence in the DEA. Rather, an assessment based upon the sufficiency of the initial obligations alone to contain file-sharing will be made by OFCOM to determine whether a technical obligation should be imposed on ISPs. This means that any anticipated technical measures will only be considered if the implementation of an initial obligations code has failed to reduce online copyright infringement by about 70 percent (Harding, 2010). Following an assessment and preparation procedure, pursuant to 124G CA 2003, it will then allow for the Secretary of State to impose an obligation on ISPs to implement technical measures (124H). The technical measures, as defined in 124G(2), are expected to be taken against some or all "relevant subscribers" (124B(3)) for the purpose of preventing or reducing infringement of copyright by means of the internet. These will include; limiting the speed or other internet capacity of the service provided to a subscriber; preventing a subscriber from using the service to gain access to particular material; suspension of service provided to a subscriber or; limiting the service provided to a subscriber in any other way. (As in 124G(3)) Section 124J, then sets out contents of code about obligations to limit internet access and so the three sections (124G, 124H, and 124J) read together therefore strengthen the Secretary of State's powers to impose technical measures on the ISPs. At this point the "suspension of services provided to a subscriber" if introduced arguably makes it on a par with HADOPI.

Furthermore, the Secretary of State may by regulation also make a provision about the granting by court of a blocking injunction in respect of a location on the internet which the court is satisfied has been, is being or is likely to be used for, or in conjunction with an activity that infringes copyright under section, 17(1), DEA. This proposed regulation then states that, an injunction may not be granted unless satisfied that it abides by the content set out within 17(4) and 17(5) DEA. The test of "is being or is likely to be used" within section 17(1) may be broad,

given that section 17(4), provides an extension of an injunction to apply not only to content hosting sites, but also to access facilitators. While this may sit in well with the goal of prohibiting access to specific file-sharing linking sites, such as BitTorrent sites, the section contains vague interpretation of the types of website that the provision is restricted to, leading to the possibility of non-infringing sites also being subjected to injunction within the meaning of section 17 DEA, should the need arise. This route, if pursued, will no doubt also represent a proportionality problem.

### **The tension in ISP obligation**

It has been noted that especially since 2007, the growing encouragement of the GRM has been at the forefront of the international lobbying campaign being waged by digital right holders to address illegal file-sharing. It does also suggest an attempt to legalise the right to monitor, while also affirming the principles that copyright should be respected and infringement punished (Rayna and Barbier, 2010) Right holders may have hoped for routine monitoring of infringing activities by ISPs as an integral part of service without the need for right holders' intervention or possibly a judicial system (Edwards, 2008), and if that could have been achieved, it would potentially reduce the costs of pursuing file-sharers. (Rayna and Barbier, 2010) However, and also as expected, this "GRM crusade" has brought tensions between digital right holders and ISPs on various fronts, not least an uneasy relationship between ISP immunities and copyright law enforcement which then begs the question as to whether or not, ISPs should be "responsible for the actions of their subscribers" (Baskerville & Baskerville, 2010, pp; 496).

ISPs have been made responsible for their users' behaviour especially with issues relating to criminal activities, but have been somewhat reluctant, possibly backed by the immunities under the ECD, to comply on civil related activities in the course of their service provision except upon knowledge and/or complicity. Although, determining the "knowledge or complicity" element and how impartial or credible such evidence might be, (given that they are often produced by the copyright holders or their affiliates) is debatable. Let us now move the discussion onto assessing the scope of ISP obligation in relation to immunities under the ECD.

### **Scope of ISP obligation**

Since the ISP's role is to act as gatekeepers to the internet, they have also been exposed to increased risks in content liability hence, the search for, and the granting of immunities from liability enshrined within the ECD (Directive 2000/31/

EC). The ECD provisions therefore create a regime of defences to ISPs who transmit copyright materials and occur when an ISP establishes that they are just mere conduits, (under Article 12) are merely caching information (Article 13) or hosting information (Article 14) provided they comply with specified statutory conditions. These may be where it is established that ISPs are not involved in selecting or initiating such transmissions (Article 12(1) a-c) and act expeditiously to take down or disable access to such information upon knowledge (Articles 13 (1e) and 14 (1b)). An example of an ISP being exempted from infringement liabilities can be found in a recent decision in *Roadshow Films v iiNet, 2010 (FCA 24)* where an Australian court ruled that iiNet (An ISP) cannot be held liable for its customers' illegal movie downloading by means of the BitTorrent P2P system. This was based on the Court's findings that the ISP had not authorised any infringements and had also complied with adequate procedures to qualify for such immunities. Although, Australian judgments are not binding in the UK courts and this ruling is more one of assessing an ISP liability for authorising infringement (*CBS v Amstrad, 1988*) rather than enforcement, it perhaps set out the extent to which an ISP safe harbour based on subscribers' infringing activities could be determined. In any case, the liability exemption provided under the ECD will not affect the possibility that a court or administrative authority, in accordance with Member States' legal systems could require the service provider to terminate or prevent an infringement (Articles 12(3), 13(2) and 14(3)) In terms of any monitoring obligations, ISPs have sought refuge in Article 15(1) of the ECD in particular when such obligations may be imposed upon them. This provision specifically states that;

"Member states shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity".

Factoring this into the requirement imposed upon ISPs by sections 124A and 124B CA 2003 there has been the suggestion that this obligation potentially infringe Article 15(1) thus, if a general obligation to monitor could be established. Nonetheless, whether or not the obligation imposed upon ISPs by the DEA contested provisions amounts to monitoring has been raised in *BT Plc & Anor. v The Secretary of State* (2011) EWHC 1021, which will be examined at the end of the paper.

It is also worth pointing out that, in the event of a general obligation on ISPs to monitor being established by the DEA, there may be other compounding challenges on its enforceability given that the UK implementation of the ECD omits the terms set out in Article 15(1) and does not seem to replace them with any

similar prohibition. Possible conflicts will include whether or not the UK is fully in compliance with the applicable EU law and whether the *EMI v UPC*, (2010 E.C.D.R. 17) test would or might apply. This was an Irish case where an injunction could not be granted because an appropriate legal basis was not available under national law. While ISPs are to enjoy immunities under the ECD, copyright owners are also provided with the legal means by which to enforce their rights largely through court orders.

### Copyright holders' rights

ISPs appear to have long been immune from any such enforcement until the encouragement of the GRM, which in practical terms, see ISPs as better placed to observe and/or record users' behaviour. This notion is also emphasised by Recital 59 of Copyright Directive, 2001/29/EC, which states that;

"In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases, such intermediaries are best placed to bring such activities to an end ... This possibility should be available even where the acts carried out by intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member State".

The usual channel to achieve ISPs' disclosure of personal information has been through the Norwich Pharmacal order, following the ruling in *Norwich Pharmacal Co v Customs & Excise*, 1974 (1974 AC. 133). This line of authority allows information to be obtained from third parties which may enable the identification of wrongdoers and trace the proceeds of wrongdoing and right holders have had little problems with being granted court orders to obtain the personal data from ISPs (*Polydor v Brown*, 2005, EWHC 3191 (Ch)). In the recently contested "volume litigation" in the UK, this route was heavily pursued (Murray, 2010) which also resulted in false positives (*Media CAT Ltd v Adams & Ors* (2011) EWPC 6, para, 34) Besides, the UK E-Commerce (EC Directive) Regulations, 2002 sets out right holders' right to apply to a court for relief so as to be able to prevent infringement of rights, (see; Regulation 20) while, aspects of Article 15,(ECD) also appear to weigh in favour of the DEA obligations. Under Article 15(2);

"Member states may establish obligations for information society service providers to promptly inform the competent public authority of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities at their request, information enabling the identification of recipients of their service with whom they have storage agreements".

What may complicate this right would be whether or not right holders who seek information such as the CILs from the ISPs fit the description of a competent public authority rather than a private entity. Another right enforcement provision can be found within Article 8(d) of the IP Enforcement Directive - IPRED (Directive 2004/48/EC) which requires member states to ensure that in the context of proceedings concerning the infringement of IP rights and in response to justified and proportionate request from claimants (right holders) the competent judicial authorities may order the provision of information on the origin and distribution networks of (goods and) services which infringe IP rights. Then, Article 8(3) of the EU Copyright Directive - EUCD (Directive 2001/29/EC) also sets forth the requirement of Member States to ensure that rights holders are in the position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right. By the definition of an intermediary to cover P2P networks as well as an ISP, it therefore gives meaning to the contested injunction provisions under section 17 of the DEA.

### **Some EU developments on ISP monitoring and data disclosure**

In what was hailed as the first European court to rule on an ISP compliance with filtering orders, the Court of First Instance in Belgium in 2007 ordered the ISP (Scarlet) to block or filter out traffic on its network (*SABAM v SA Scarlet*. (2007) *E.C.D.R.* 19). This case had been brought by the Belgian authors' rights group SABAM, who believed the order was necessary to prevent infringement of its members' copyright. Although, it has been controversial from the start of the proceedings and the ruling by the Court of First Instance was believed to have impacted on the scope of ISP obligation, it could still be possible due to the diverse interpretation of implemented EU laws at national levels. Whether or not the EUCD or the IPRED superseded the ECD, the court had maintained that although the mere conduit defence was not relevant to the case, the duty imposed on the ISP still protected the mere conduit exception and that its injunction also prohibited a general obligation to monitor the network. It was to be followed by a Danish court ruling also permitting filtering, (*SONOFON A/S v IFPI Denmark* (2009) *E. C. D. R.* 10) based on its interpretation of a transposed EU law. Following on from SABAM (2007) ruling, the ISP Scarlet pursued an appeal against the verdict and successfully won a court reprieve prompting the national court to now refer questions to the ECJ (C-70/10 SABAM *Extended v Scarlet*). The guidance sought by the referral is for the ECJ to rule on whether a national court can order an ISP to install a system for filtering and blocking electronic communications in order to protect IP rights.

A recent ECJ development in the SABAM case (C-70/10 SABAM *Extended v Scarlet*) has been the Advocate General's opinion which considers that Scarlet should

not have to filter copyright-infringing traffic from its service as to do so would be a restriction on the right to respect for the privacy of communications and the right to protection of personal data, both of which are rights protected under the Charter of Fundamental Rights. This reinforces the view that whereas IP is a property right, data protection being related to privacy is more akin to a human right. And by the same token, (according to the opinion) the deployment of such a system would restrict freedom of information, which is also protected by the Charter of Fundamental Rights (ECJ Press Release, 2011). The implication of the Advocate General opinion (if followed in the judgment) will complicate efforts by right holders to secure “rubber-stamped” monitoring obligation by ISPs through court orders. Furthermore, this opinion, if followed, would also suggest the importance of, at least, enabling the ECD and EUCD to complement each other rather than the EUCD superseding the ECD as was largely thought to have been the issue in the SABAM 2007 ruling.

In relation to personal data disclosure, the ECJ judgments in the *Tele2* (2009) and *Promusicae* (2008) cases provided some neutral interpretations. Although these decisions appeared vague and left the balancing exercise to be completed by the national courts, they have stressed the need to balance both copyright and the rights of consumers through the application of national laws by Member States. In the *Tele2* case (C-557/07) *LSG v Tele2*, it was held that the Community provisions (Article 8(3) of Directive 2004/48/EC and Article 15(1) of Directive 2002/58/EC) do not preclude Member States from imposing an obligation to disclose third parties' personal data to enable civil proceedings for copyright infringements. It then stated the need for any applicable law being transposed into national laws, to comply with the balancing of the fundamental rights involved while also considering the general principles of Community law such as the principle of proportionality. The ECJ in *Promusicae* (C-275/06 *Promusicae v Telefonica*), was also confronted with the consideration of the application of a number of directives and separate provisions to provide clarity on the balancing of rights. Here, the ECJ recognised that any obligation to disclose personal data had to be in order to ensure the effective protection of copyright in the context of civil proceedings. The Court also recognised that any obligation to disclose confidential personal data must then respect Articles 7 and 8 of the Charter of Fundamental Rights that require protection for the right to respect for family and private life and the right to the protection of personal data. The ECJ then held that when implementing such directives, laws must be interpreted by national courts and authorities in a manner consistent with the directives but not to rely on an interpretation which conflicts with these rights as well as considering the principle of proportionality.



It could be deduced from the outcome of both cases (*Tele2* and *Promusicae*) that as long as the general principle of proportionality and the balancing of rights can be considered at the national level, the disclosure of personal data in civil cases to enforce property rights is at least permissible. This may then justify efforts by the right holders to actively engage in identity disclosure procedures in response to copyright infringement within the meaning of the DEA obligations, although users' privacy and data protection concerns have also emerged. Furthermore, the reliance on national laws with its vast number of optional exceptions within implemented directives then means Member States can pick and choose at will, which consequentially also impact on efforts at EU harmonisation of rights. Before moving on to the evaluation of relationships between ISPs and right holders and possible implications from recent developments on ISP obligations, some aspects of proportionality needs to be highlighted in the context of the DEA provisions.

### The Proportionality Debate

In assessing proportionality, several issues may be considered. This may include whether or not the DEA contested provisions are set out to specifically achieve the goal of reducing illegal file-sharing or exceed its mandate, whether they are necessary and appropriate, or how far it encroaches on consumer rights. More importantly, the impact of a technical measure where subscribers (or innocents sharing the same account) could be deprived of their internet access continues to form a major part of the proportionality debate and violation of subscribers' fundamental rights.

Such uneasiness, among other things, prompted a recent judicial review of the DEA by the UK High Court, demanded by two of UKs biggest ISPs (BT and TalkTalk) who wanted clarity and certainty on the law before its implementation. The High Court then agreed to review the law to see whether the DEA conflicted with EU laws on privacy and ISPs' liabilities for users' behaviour (Ashton, 2010). At the hearing, five grounds of challenge were advanced by the Claimants in respect of the contested provisions which related to the EU's Technical Standards Directive, (TSD) the Authorisation Directive, (AD) the E-Commerce Directive, the Privacy and Electronic Communications Directive and on the proportionality principle. In the Court's judgment, all but one of the challenges advanced were dismissed, indicating that the directives had not been breached and at least the DEA, as it stands, is proportionate (*BT Plc & Anor. v The Secretary of State* (2011) EWHC 1021). Although in the context of this paper, aspects of TSD and AD are not discussed. In terms of the necessity of the DEA provisions, arguably copyright needs to be protected hence various provisions within national and EU laws to order ISP compliance with IP enforcement online. The mere-conduit provi-

sion (Article 12 ECD) being one of ISP defences could be interpreted as striking a careful balance between the different interests involved, given that ISPs are free to provide services to their subscribers but then to also cooperate with copyright enforcement when prompted to do so (*BT Plc & Anor. v The Secretary of State* (2011) EWHC 1021).

Another area of concern by the interveners related to why an existing line of authority such as a Norwich Pharmacal line of authority is not used as perhaps a less restrictive option. This preference therefore also required a comparison to be made between this order and the DEA obligations. Assuming that the Norwich Pharmacal order is less restrictive, it could also be more intimidating in that, once a subscriber's identity has been disclosed by the ISP, the usual form of contact with the alleged infringer is a so-called "speculative invoice" seeking immediate financial compensation for which in the case of default, court proceedings are the only alternative. This may not be the same with the DEA where, the processes set out in the obligations code begins with a notification(s) alongside education to assist the alleged subscriber to desist, secure subscription account and opt for a legal alternative. While a technical obligation within the DEA will only be considered and scrutinised before its introduction or may never be introduced if the initial obligation alone accomplishes the set goal. The classical proportionality question then will be whether or not even a less restrictive measure achieves the same objective?

The judicial review judgment had also sought to justify the lengthy consultation processes which took into account representations by all stakeholders to have resulted in a balance being struck with all interested parties before its enactment hence, proportionality considered (*BT Plc & Anor. v The Secretary of State* (2011) EWHC 1021, para, 212). Although, there could be a potential risk of a "chilling" effect arising from the introduction of a technical measure, since the measures are not even operational and hence no accumulation of experience of their effects in practice, it would be premature to conclude the impact of any chilling effect from a measure that is yet to be implemented (*BT Plc & Anor. v The Secretary of State* (2011) EWHC 1021, para, 240). In any case, if a technical measure will be introduced to include the termination of internet access, it is bound to clash with aspects of users' human rights as recently reported (La Rue, 2011).

### **The judicial review judgment – Any clarity?**

In order to measure whether or not the recent judicial review judgment provides any clarity on the ISP obligations, we would perhaps be reminded that, while general monitoring of subscribers conflict with the earlier measures, (see Article

15(1) ECD) specific monitoring seems to be supported and emphasised by Recital 47 of the Directive. As it states:

“Member states are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation”.

This then shift the focus onto what kind of obligation the DEA provisions propose, pursuant to 124A and 124B CA 2003. It could be assumed that the initial obligations does suggest nothing more than a specific obligation between ISPs and other parties. Whether or not such obligations can be regarded as monitoring has required urgent clarification and which seems to have been given in (*BT Plc & Anor. v The Secretary of State* (2011) EWHC 1021). The judgment found that the DEA imposed no general obligation on the UK participating ISPs to monitor any information, nor a general obligation to actively seek facts or circumstances indicating illegal activity (Article 15(1) ECD).

The Court sought to clarify that the CIR data to be handled by the ISPs (under 124A CA, 2003) will be nothing more than merely reporting to the subscriber, information received from the right holders of alleged infringement. While the maintenance of the CILs by ISPs, (124B CA, 2003) will also amount to a mere compilation of CIRs in respect of a repeat infringer, rather than an obligation to monitor that information. The Court, emphasising no breach of Article 15(1) ECD also pointed out that, right holders have been the parties who actively seek facts and circumstances indicating illegal activity through the harvesting of IP addresses of alleged infringers, as prescribed by the DEA. In other words, it is the copyright owner, rather than the ISP who conducts the (monitoring) investigation and the CIR becomes a work product of another party, while the CIL is simply a compilation of such reports in respect of the relevant subscriber (See *BT Plc & Anor v. Secretary of State* (2011) EWHC 1021, para 116-118). Now, how do the recent developments in both the DEA review and the consideration of the SABAM case by the ECJ impact or affect ISPs responsibilities for users behaviour?

### **Possible Implications and Directions?**

Based on the judgment in, *BT Plc & Anor v Secretary of State* (2011) EWHC 1021, and assuming that an appeal which is now being sought by Claimants (BT Press Release, 2011) does not alter this ruling, an interesting interpretation would have emerged about the responsibility of ISPs under a GRM. The ruling as it stands establishes that the DEA imposes no general obligation on ISPs to monitor hence especially the ECD is not breached and the DEA is lawful. On the other hand, if

the recent Advocate General's opinion in *SABAM* (C-70/10) is followed in the ECJ judgment, it may be that the installation of systems (at issue) by the ISP *Scarlet*, would potentially filter all data communications passing via *Scarlet*'s network in order to detect copyright infringing data which in the Advocate General opinion, will constitute a general obligation to monitor and hence will be in breach of the fundamental rights of subscribers (ECJ Press Release, 2011).

In summing up the implications and possible direction of the responsibilities imposed on ISPs vis à vis their subscribers, there is the indication that a GRM such as the one legislated by the DEA, (involving third parties tasked with investigating infringement) may not hinder ISP obligations to comply and cooperate with right holders and in fact be legal. Whereas, if the court imposes a direct order on ISPs to install monitoring systems to filter and block content, (absent other investigating parties) a general obligation to monitor may be established which would potentially be in breach of subscribers' fundamental rights and therefore unenforceable, as the Advocate General has suggested. Importantly, it is worth mentioning that these developments may still not hinder a national court's power to impose more specific obligations on intermediaries, and it is hoped that the ECJ judgment in *SABAM* (C-70/10 *SABAM Extended v Scarlet*) will eventually help clarify aspects of ISP obligations in addressing copyright infringements.

## Conclusion

In assessing the goals of the DEA online copyright infringement provisions, it is becoming increasingly essential for right holders to require access to a trail of evidential materials kept by the ISP, when internet is accessed so as to enable the enforcement of their rights and especially when fighting illegal file-sharing. These efforts, despite successes through the use of Norwich Pharmacal orders and currently with the GRM, has also kept users' confidentiality and right to privacy debates alive requiring clarity on the balancing of rights as well as the need for rules on copyright and e-commerce to complement each other. On the principle of proportionality, it appears that, a vivid assessment of its impact in relation to the DEA may still be contingent on the Code taking legal effect as the initial obligation may or may not trigger a technical obligation. While, ISPs sit in between subscribers and copyright enforcers, there appears to be a very difficult task to accomplish, not least, having to deal with the somewhat uneasy relationship between the immunities under the ECD and the responsibilities under copyright law. Also, as the internet arguably shifts from being a luxury into a right, governments are faced with the complicated task of achieving an ostensibly impossible middle-ground in satisfying both the copyright holder and consumers. Perhaps there is the need for any copyright enforcement to take into account the importance of ISP immunities and fundamental values of the end-users when achieving

such goals given that the ISP's primary responsibility is to provide a transit service to its subscribers by its role as a gatekeeper to the Internet.

## References

### Books

Baskerville, D. & Baskerville, T. (2010), *The music business handbook and career guide*. 9th Edition. Sage Publication.

Casey, T. (2001) *ISP Liability: survival guide, strategies for managing copyright, spam, cache and privacy regulations*. John Wiley & Sons.

Edwards, L. and Waelde, C. (2009), *Law and the Internet*. Hart Publishing. Oxford.

Lim, Y. (2007) *Cyber law: commentaries and materials*. 2nd Edition. Oxford University Press.

### Cases

*A&M Records Inc v. Napster, Inc* 239 F.3d 1004 (9th Cir. 2001).

*Ashdown v. Telegraph Group Ltd*, (2001) EWCA Civ 1142.

*Bonnier Amigo Music Norway AS v. Telenor Telecom Solutions AS* (2010) E.C.D.R. 2.

*British Telecommunications Plc & Anor. R. (on the application of) v. The Secretary of State for Business, Innovation and Skills* (2011) EWHC 1021(Admin).

Case – C-275/06 *Productores de Musica Espana v. Telefonica* (2008) 2 C.M.L.R. 17.

Case – C-557/07 *LSG Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH* (2009) OJC 113/14.

Case – C-70/10 *Scarlet Extended SA v. SABAM* OJ (2010) C 113/30.

*CBS Songs Limited v. Amstrad Consumer Electronics Plc* (1988) 2 WLR 1191.

*Durant v. FSA*, (2003) EWCA Civ. 1746, Court of Appeal (Civil Division).

*EMI (Ireland) Ltd v. Eircom Ltd* (2009) IEHC 411 (HC Irl).

*EMI (Ireland) Ltd v. Eircom Ltd* (2010) IEHC 108 (HC Irl).

*EMI Records (Ireland) and Others v. UPC Communications Ireland Ltd* (2010) E.C.D.R. 17.

*Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259 (9th Cir. 1996).

*Media CAT Ltd v. Adams & Ors* (2011) EWPCC 6.

*Metro-Goldwyn-Mayer Studios v. Grokster Ltd*, 125 S. Ct. 2764 (2005).

*Norwich Pharmacal Co v. Customs & Excise*, (1974) AC. 133.

*Polydor Limited and Others v Brown and Others*, (2005) EWHC 3191 (Ch).

*Roadshow Films Pty Ltd v. iiNet Limited*, (2010) FCA, 24.

*SABAM (Societe Belge des Auteurs, Compositeurs et Editeurs) v. SA Scarlet*. (2007) E.C.D.R. 19.

*Shapiro, Bernstein and Co. v. H.L. Green Co.*, 316 F. 2d 304 (2d Cir. 1963).

*SONOFON A/S (formally DMT2 A/S) v IFPI Denmark* (2009) E. C. D. R. 10.

*Totalise PLC v. Motley Fool Ltd & Another*, (2001) EWCA Civ 1897.

*Twentieth Century Fox Film Corporation v Newzbin Ltd* (2010) EWHC 608 (Ch).

### ***Legislation/Directives/Conventions***

Authorisation Directive (Directive (2002/20/EC).

Charter of Fundamental Rights of the European Union, (2010/c 83/02).

Digital Millennium Copyright Act (DMCA).

Electronic Commerce Directive (Directive 2000/31/EC).

Privacy and Electronic Communications Directive (Directive 2002/58/EC).

The Copyright, Designs and Patents Act (CDPA) 1988 (c. 48).

The Data Protection Act, 1998.

The Data Protection Directive (Directive 95/46/EC).

The Digital Economy Act, (2010) Chapter 24.

The Electronic Commerce (EC Directive) Regulations 2002, (SI 2002/2013).

### ***Journals***

De Beer, J. and Clemmer, C. (2009) Global trends in online copyright enforcement: a non-neutral role for network intermediaries? *Jurimetrics Journal*, 49, 375-409.

Harding, T. (2010) The digital economy Act, 2010: content and implications. *Journal of E-Commerce Law and Policy*, 12 (5), 3-5.

Lambrick, J. (2009) Piracy, file sharing ... and legal fig leaves. *Journal of International Commercial Law and Technology*, 4 (3), 185-195.

Ucchi, N. (2011) *Cardozo Journal of International and Comparative Law (JICL)*, Vol. 19, 2011, 1-28.

Luck, M. (2009) Internet policing and regulation. *Journal of E-Commerce Law and Policy*, 11 (6), 3.

May, B. and Liens, M. (2009) France's attempt to introduce anti-piracy legislation. *Journal of E-Commerce Law and Policy*, 11 (7), 10-12.

Philips, J. (2009) Three strikes' ... and then? *Journal of Intellectual Property Law & Practice*, 4 (8), 521.

Rayna, T. & Barbier, L (2010) Fighting consumer piracy with "graduated response": an evaluation of the French and British implementations. *International Journal of Foresight and Innovation Policy*, 6 (4), 294-314.

Weston, M. (2010) DEA 2010: Wi-Fi Liability. *Society for Computers and Law* 21 (3), 31-33.

Yu, P. (2010) The "graduated response". *Florida Law Review*, 62, 1373-1430.

### **Internet**

Anderson, N. (2008) RIAA "graduated response" plan: Q&A with Cary Sherman. Online at <<http://arstechnica.com/old/content/2008/12/riaa-graduated-response-plan-qa-with-cary-sherman.ars>>. Accessed: 23.01.2011.

Anderson, N. (2009a) Irish ISP agrees to disconnect repeat P2P users. Online at <<http://arstechnica.com/telecom/news/2009/01/irish-isp-agrees-to-disconnect-repeat-p2p-users.ars>>. Accessed: 03.02.2011.

Anderson, N. (2009b) Verizon to forward RIAA warning letters (but that's all). Online at <<http://arstechnica.com/tech-policy/news/2009/11/verizon-to-forward-riaa-warning-letters-but-thats-all.ars>>. Accessed: 13.02.2011.

Anderson, N. (2010) Cor blimey! British ISPs must fund P2P copyright crackdown Online at <<http://arstechnica.com/tech-policy/news/2010/09/should-isps-pay-for-p2p-warning-letters-uk-says-yes.ars>>. Accessed: 01.02.2011.

Arthur, C. (2011) ACS: law and mediaCAT close their doors, ending file sharing claims. Online at <<http://www.guardian.co.uk/technology/blog/2011/feb/04/acs-law-mediakat-close-filesharing>>. Accessed: 07.02.2011.

Ashford, W. (2010) ACS law hacking a text-book case that exposes several weaknesses. Online at <<http://www.computerweekly.com/blogs/read-all-about-it/2010/09/acs-law-hacking-a-text-book-ca.html>>. Accessed: 19.01.2011.

Ashton, R. (2010) DEA goes to judicial review. Online at <<http://www.musicweek.com/story.asp?sectioncode=1&storycode=1043241>>. Accessed: 15.11.2010.

BT Press Release (2011) BT and TalkTalk appeal Digital Economy Act judgment. Online at <<http://www.btplc.com/News/Articles/ShowArticle.cfm?ArticleID=A057B5E1-1BB3-4751-B208-60EC04E1E348>>. Accessed: 01.06.2011>.

Camphuizen, A. (1999) Telco's ISP ADDS Filter Technology. Online at <http://www.internetnews.com/bus-news/article.php/216671/Telcos-ISP-Adds-Filter-Technology.htm>. Accessed: 17.03.2011.

Cardingham, C. (2008)) £16,000 (\$32,000) fine for first brit convicted of illegal file sharing. Online at <<http://www.money.co.uk/article/1001203-16-000-pound-fine-for-first-brit-convicted-of-illegal-file-sharing.htm>>. Accessed: 12.01.2011.

Cellan-Jones, R. (2009) Fact about file-sharing. Online at <[http://www.bbc.co.uk/blogs/technology/2009/11/facts\\_about\\_filesharing.html](http://www.bbc.co.uk/blogs/technology/2009/11/facts_about_filesharing.html)>. Accessed: 11.03.2011.

Cheng, J. (2009) Germany says "Nein" to three-strikes infringement plan. Online at <<http://arstechnica.com/tech-policy/news/2009/02/germany-walks-away-from-three-strikes-internet-policy.ars>>. Accessed: 26.01.2011.

Dickerson, J. and Watson, A. (2010) Commentary by Burges and Salmon (LLP) on The Digital Economy Act, 2010. Online at <[http://www.burges-salmon.com/Sectors/technology\\_media\\_telecommunications/Publications/The\\_Digital\\_Economy\\_Act\\_2010.pdf](http://www.burges-salmon.com/Sectors/technology_media_telecommunications/Publications/The_Digital_Economy_Act_2010.pdf)>. Accessed: 15.02.2011

Du Preez, D. (2011) Government says ISPs should quit bellyaching about Digital Economy Act. Online at <<http://www.computing.co.uk/ctg/news/2025804/government-isps-quit-bellyaching-digital-economy-act>>. Accessed: 15.02.2011

ECJ Press Release (2011) Advocate General's Opinion in case C-70/10 Scarlet Extended v Société belge des auteurs compositeurs et éditeurs (Sabam) Online at <http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-04/cp110037en.pdf>. Accessed: 15.04.2011

Edwards, L. (2009) Mandy and me: some thoughts on the Digital Economy Bill. Online at <<http://blogsript.blogspot.com/2009/11/mandy-and-me-some-thoughts-on-digital.html>>. Accessed: 14.01.2011.

Fiveash, K. (2011) Online at OFCOM to review Digital Economy Act site-blocking measures. <[http://www.theregister.co.uk/2011/02/01/OFCOM\\_reviews\\_digital\\_economy\\_act/](http://www.theregister.co.uk/2011/02/01/OFCOM_reviews_digital_economy_act/)>. Accessed: 02.02.2011>.

Fleischer, P. (2007) Are IP addresses "personal data"? Online at <<http://peterfleischer.blogspot.com/2007/02/are-ip-addresses-personal-data.html>>. Accessed: 23.03.2011>.



Forde, E. (2010) France's 'three strikes' Law Goes into action. Online at <<http://www.musicweek.com/story.asp?storyCode=1042612&sectioncode=1>>. Accessed: 12.02.2010.

Geist, M. (2010) Estimating the cost of a three-strikes and you're out system. Online at <<http://www.thestar.com/business/article/755443-geist-three-strikes-and-youre-out-system-draw-cries-of-foul-from-governments>>. Accessed: 11.03.2011.

Horten, (2009) HADOPI-2 goes to Constitutional Council. Online at <[http://www.iptegrity.com/index.php?option=com\\_content&task=view&id=417&Itemid=9](http://www.iptegrity.com/index.php?option=com_content&task=view&id=417&Itemid=9)>. Accessed: 10.03.2011>.

Hunton and Williams, (2010) Study on online copyright enforcement and data protection in selected member States, European Commission, DG Internal Market and Services. Online at <[http://ec.europa.eu/internal\\_market/iprenforcement/docs/study-online-enforcement\\_042010\\_en.pdf](http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_042010_en.pdf)>. Accessed: 14.02.2011

Killock, J. (2010) The future of the Digital Economy Act is in your hands. Online at <<http://www.openrightsgroup.org/blog/2010/the-future-of-the-digital-economy-act-is-in-your-hands>>. Accessed: 10.02.2011>.

La Rue, F. (2011) Report of the special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Online via [http://torrentfreak.com/un-disconnecting-file-sharers-breaches-human-rights-110603/?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+Torrentfreak+%28Torrentfreak%29](http://torrentfreak.com/un-disconnecting-file-sharers-breaches-human-rights-110603/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Torrentfreak+%28Torrentfreak%29). Accessed: 07.06.2011

Leppla, F. (2010) Tens of thousands could be priced out of broadband after government announcement on file sharing code. Online at <<http://www.openrightsgroup.org/blog/2010/tens-of-thousands-could-be-priced-out-of-broadband-after-government-announcement-on-file-sharing-code>>. Accessed: 04.02.2010

Llewellyn, H. (2009) 'three-strikes' off anti-piracy agenda in Spain. Online at [http://www.billboard.biz/bbbiz/content\\_display/industry/e3i8071e0d9c25-cb6b876d3771fb7e3d102](http://www.billboard.biz/bbbiz/content_display/industry/e3i8071e0d9c25-cb6b876d3771fb7e3d102). Accessed: 02.01.2011

Lovejoy, N. (2011) Procedural concerns with the HADOPI "graduated response" Model Online at <<http://jolt.law.harvard.edu/digest/copyright/procedural-concerns-with-the-HADOPI-graduated-response-model>>. Accessed: 15.01.2011

Mann, A. (2010) The Digital Economy Bill. Online at <<http://www.bristows.com/?pid=46&nid=1491&level=2>>. Accessed: 22.01.2011

Moya, J. (2010) Finland makes Internet access a fundamental right. Online at <<http://www.zeropaid.com/news/89772/finland-makes-internet-access-a-fundamental-right/>>. Accessed: 23.03.2011>.

Petrou, A. (2010) Coalition government u-turns on repealing Digital Economy Act. Online at <<http://www.techeye.net/internet/coalition-government-u-turns-on-repealing-digital-economy-act>>. Accessed: 14.02.2011>.

Pilcher, P. (2010) So long Section 92A - new Copyright Bill revealed. Online at <<http://www.nzherald.co.nz/technology/news/article.cfm?cid=5&objectid=10628193>>. Accessed: 22.01.2011.

Singel, R. (2008) Internet mysteries: how much file-sharing traffic travels the net? – Update. Online at <<http://www.wired.com/threatlevel/2008/05/how-much-file-s/>>. Accessed: 20.12.2010.

Sroussi, G. (2009) France - The HADOPI law and France's controversial fight against piracy. Online at <<http://www.linklaters.com/Publications/Publication1403Newsletter/20091016/Pages/FranceTheHADOPILaw.aspx>> Accessed: 14.02.2011.

Strowel, A. (2009) Internet piracy as a wake-up call for copyright law makers - Is the “graduated response” a good reply? The WIPO Journal, 2009 Issue: 1. pg; 83-94 Online at [http://www.world-intellectual-property-organization.com/about-wipo/en/pdf/wipo\\_journal.pdf](http://www.world-intellectual-property-organization.com/about-wipo/en/pdf/wipo_journal.pdf). Accessed: 23.01.2011>.

Topware Interactive v Barwinska. (2008) Patents county Court's partial copy of the order (PAT-08023) Online at <<http://beingthreatened.yolasite.com/resources/Beschluss%20Topware%20Interactive%20INC.pdf>>. Accessed: 01.02.2011>.

TorrentFreak, (2010) France starts reporting ‘millions’ of file-sharers. Online at <<http://torrentfreak.com/france-starts-reporting-millions-of-file-sharers-100921/#>>. Accessed: 22.01.2011.

TorrentFreak, (2011) RIAA labels Spain and Canada as piracy havens. Online at <<http://torrentfreak.com/riaa-labels-spain-and-canada-as-piracy-havens-110217/>>. Accessed: 17.02.2011.

Williams, C. (2010) High Court to probe Digital Economy Act. Online at <[http://www.theregister.co.uk/2010/11/10/bt\\_talktalk\\_digital\\_economy/](http://www.theregister.co.uk/2010/11/10/bt_talktalk_digital_economy/)>. Accessed: 22.01.2011.

### ***Official Publications (Online)***

Article 29 Data Protection Working Party (2007) Opinion 4/2007 on the concept of personal data. Online at <[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf)>. Accessed: 30.03.2011>.

BIS (2010) HM Government response to the consultation on online infringement of copyright (Initial Obligations) cost sharing. Online at <<http://www.bis.gov.uk/assets/biscore/business-sectors/docs/o/10-1131-online-copyright-infringement-government-response>>. Accessed: 14.02.2011>.

Carter, S. (2009) The Digital Britain Report. Online at <<http://webarchive.nationalarchives.gov.uk/+<http://www.culture.gov.uk/images/publications/digitalbritain-finalreport-jun09.pdf>> Accessed: 02.12.2010.

Digital Economy Act, 2010. Chapter 24. Online at <<http://www.legislation.gov.uk/ukpga/2010/24/data.pdf>>. Accessed: 03.01.2011>.

DSI - Draft Statutory Instrument (2011 No. 0000) The online infringement of copyright (Initial Obligations) (Sharing of Costs) order 2011. Online at <<http://www.legislation.gov.uk/ukdsi/2011/9780111505779/contents>>. Accessed: 25.01.2011.

Gowers Report, (2006) Online at <<http://www.officialdocuments.gov.uk/document/other/0118404830/0118404830.pdf>>. Accessed: 01.02.2011.

Information Commissioner Office (ICO) (2010) Data Protection: Personal information Online – Code of Practice. Online at <[http://www.ico.gov.uk/for\\_organisations/data\\_protection/topic\\_guides/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/personal\\_information\\_online\\_cop.ashx](http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~media/documents/library/Data_Protection/Detailed_specialist_guides/personal_information_online_cop.ashx)>. Accessed: 22.02.2011>.

Parliamentary Debate, (2010). The Digital Economy Bill Online at <<http://www.parliamentlive.tv/main/player.aspx?meetingid=6118&st=15:28:3>>. Accessed: 20.03.2011.

UN General Assembly Human Rights Council Report (2011) Online via <[http://torrentfreak.com/un-disconnecting-file-sharers-breaches-human-rights-110603/?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed%3A+Torrentfreak+%28Torrentfreak%29](http://torrentfreak.com/un-disconnecting-file-sharers-breaches-human-rights-110603/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Torrentfreak+%28Torrentfreak%29)>. Accessed: 07.06.2011>.

### ***Podcast***

Walden, I. (2011) Investigations & enforcement: the role of Internet Service Providers <http://www.cpdcast.com/podcasts/investigations-and-enforcement-the-role-of-isps>.

# When Personalization Becomes Too Personal

---

---

Christina Gkarnara

---

---

## 1. Introduction

With the advent of the WWW the number of users who interact with search engines increases rapidly as rapidly flourish the documents that are indexed by search engines. Users can find the desirable data in two predominant ways: they can either *search* or *browse* [18]. Via the first way, users submit a keyword to a search engine, which retrieves documents that contain these keywords. This way is the most popular way to seek information and the advantage is that the user finds quickly the information by identifying the pages which contain the information query [17]. The second way is by browsing and is done through an existing ontology of topics on which user navigates by clicking the preferred topical node until he reaches the desirable area of interests [18]. This way of seeking information is efficient when the user isn't connoisseur of the search domain. The Web is an information repository in which the data structure is heterogeneous. Many times users resent by the numerous unrelated results that search engines retrieve thus making the user's navigation a time consuming procedure.

To fill this void, personalization of search results has been introduced as a promising direction in enhancing the accuracy of the retrieved results in terms of user-specific needs. Personalized search targets to design systems which retrieve tailored collections of pages adaptable to each individual user profile. There exist two approaches to construct the user's profile, through *explicit* or through *implicit* feedback [17]. Both ways require collecting and storing user information which illustrate the users interests, preferences, needs, tastes and general users personal data in order to decipher the query intention. Hence, in order to achieve search personalization, search engines need to collect large amounts of users' personal data. But, users are reluctant to reveal private information or their preferences and often are concerned about their privacy breach. In this article, we survey privacy issues pertaining to web search that have been identified by numerous researchers and we highlight the avenues for future research on maintaining profile privacy in personalized web search. The quest of our survey is to demonstrate how users can achieve a balance between personalized and secured search results.

The article is organized as follows. In Section 2, we highlight the contribution of personalization when searching the Web. In Section 3, we present the two approaches that exist to obtain personalization and we introduce the concerns they raise on privacy issues. In Section 4, we underline how to achieve privacy in web search by presenting existing approaches. In Section 5, we list some challenges that need to be addressed and in Section 6 we conclude the article.

## 2. The Contribution of Personalization

Search engines have been designed to gratify different users and meet their growing needs and expectations while they seek for information. Despite the advancement of web search, search engines are still not optimally operant. This is due to the following: firstly, queries might be polysemous [21]. When different information seekers submit the same query in a search engine, each of them expects dissimilar retrieved results. For, example, for the query “cookies”, some users desire to inform about the mechanism that text files are storing on the client side computer, while others expect information related to the dessert and how to cook the dessert “cookies”. Another example, for the query “java”, some users desire to inform about the programming language “java”, while others expect information related to “coffee” [21]. Therefore, the second problem that emerges is that the search engines for every input information query like above retrieve the same information to all users, is that they follow the model of “one size fits all” [17]. This model makes the user’s navigation through the retrieved results until reaching to the desired information a time consuming procedure.

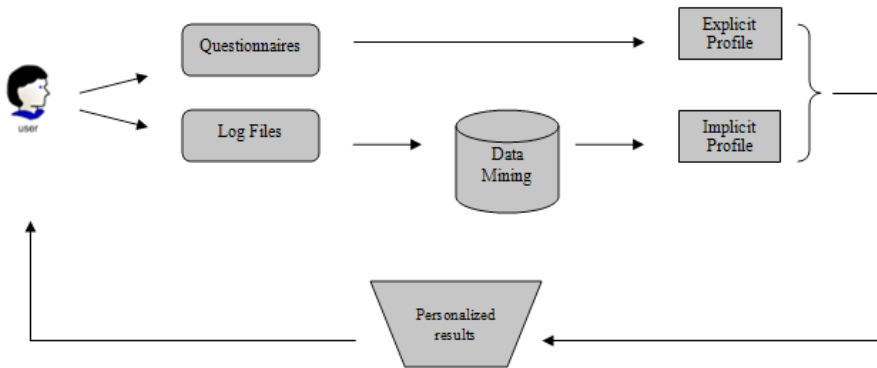
To overcome the above, we can personalize search results according to user-specific needs. Personalized search targets to design systems which retrieve tailored collections of potentially relevant pages classified in such a way that reflects the pages relevance to the query keywords and to be adaptable to each individual users profile [17]. In order to achieve personalization, systems need to construct a user profile which represents the user’s interests and preferences. The approaches towards identifying user profiles are discussed in the section 3. One example to illustrate the contribution of personalization is referred in [20]. The system called “Susanna” affords the opportunity to a user to adopt on its own the navigational pattern he desires. Namely, the system gives the opportunity to the user to choose if he wants to retrieve personalized results or not. Assuming there are two users each of them wishes to get personalized results and they both issue the same query, e.g. searching for a book and especially a book written by an author named King. In the case of the first user who doesn’t want personalized results, the system retrieves results which contain books of the author Stephan King which they don’t belong into a specific thematic hierarchy. In the case of the second user who desires personalized results, before issuing the query, he de-

clares to the system his interests and preferences and the system constructs a user profile. When the user inputs the same query, the system retrieves personalized results and particularly the system retrieves results which contain books of the author Robert King that belong to a particular thematic hierarchy which is "Computers & Web". Thus the second user saves time and gets the desirable results in a more effective and efficient manner. Consequently, the contribution of personalization is manifold and the essential prerequisite to achieve personalization is the construction of user search profiles. In the next section, we present the two main approaches towards creating search profiles.

### 3. Approaching Personalization

This section focuses on personalization approaches and in particular on the two main directions via which user profiles are constructed. Figure 1 illustrates the overall search personalization process for both of the presented ways. The first approach of user modeling is the technique of *explicit profiling* [17]. The user's profile is constructed via the explicit declaration of preferences, usually through registration forms or questionnaires. Hence, the interests of each individual user can be identified. The system which implements the explicit approach requires the direct involvement of the users. The drawback of this approach is that the disclosure of personal data makes the users disinclined to explicitly specify their needs and they find the registration a time consuming and confusing task. The second approach of user modeling is through *implicit profiling* [17]. To overcome the challenges of the explicit feedback, the implicit profiling does not require the user's direct involvement. The user's profile is constructed by tracking and monitoring the user's querying and results' navigational behavior. The systems which implement the implicit approach capture the personal needs of each specific user via the interaction among a user and the system. Particularly, by capturing the complete navigational path such as the pages the user visits, the URLs and anchor texts the user follows for particular queries, the time and date of access [17].

Thus, the system emanates the user's interests in personal topics and constructs the profile. An overview of above can be found in [2,3,4,8,14,23,24].



**Figure 1.** Explicit & Implicit Profiling to learn and capture user's interests to retrieve personalized results.

Implicit profiling relying upon the recorded users' interaction with the search engine is effective in that it does not interfere directly with the user. Still, it raises concerns about the level of distribution and privacy of the collected data. Such data concern the full record of the user's search logs. A current example of data disclosure is the case of AOL search engine [1,27,15]. In August of 2006, the American Online (AOL) search engine disclosed an extremely large amount of query log. This query log extracted over a period of three months. 20 million search queries which have been submitted by 658,000 users were released in order to help researchers in the Information Retrieval (IR) community. This release denotes expose of private data for a number of AOL users. The mistake of the AOL search engine was that they haven't sanitized the queries; they have just replaced the user IDs but not the search queries. For example, journalists from New York Times (not professionals specialized in data mining) could accomplish to decipher the user corresponding to ID 4417749, even without taking account the existence of social security numbers, driving license numbers and credit card numbers. Through observation the detailed and multiple queries they found that the user with the ID 4417749 was corresponded to a 62 year old woman living in Georgia. Another example [27] is the search queries entered by the user 1515830:

*calories in bananas*  
*surgical help for depression*  
*jobs in denver colorado*  
*teaching positions in denver colorado*  
*anti psychotic drugs*

As the above studies suggest, it is relatively easy to decipher private information about concerns the user such as health and mental condition, profession, geographical location. We can comprehend through this example how users unintentionally reveal information about themselves when submitting queries in search engines. Beyond the analysis of user's search logs, another way a search engine can identify the user is under their IP address. In order for a user to communicate and interact with search engines, an IP address is indispensable. An IP address is a unique string of numbers assigned to each user's computer. In short, IP is like a user's street address or telephone number. Furthermore, "cookies" enable search engines to decipher a user like a recurrent visitor and glean his searches and store them even using different IP address [27]. From the above we understand that users are treated as easy prey. Most information seekers are concerned about their privacy and they desire safety and security during their navigation. In the next section, we discuss technological approaches that have been researched so as to enhance users' privacy protection and accomplish a balance between effective personalization and privacy protection.

#### **4. How to achieve privacy in personalized web search**

In the current section we present a bibliographic overview of the technical solutions that have been examined in order to account for privacy issues with respect to personalization. Privacy Enhancing Technologies have been deployed since early eighties. Recent surveys indicate that although nearly 80% of the information seekers are interested in personalization [16], 83% of them are concerned about the privacy of their personal data, 82% refuse to disclosure personal information to a web site, 27% are not inclined to provide any personal information to a web site, 34% of the information seekers submit false information when asked to register or fill out an online form and 49% believe that sites share users' personal information with other sites, thus resulting to privacy breach [26]. Users differ from one another, which indicates that every user has different requirements for privacy protection and as such their opinions on privacy enhancement differ widely. There are users who don't desire to share personal information with anyone, while others are eager to disclosure personal information in order to achieve high quality services. The level of privacy protection depends on the individual needs and expectations [13] and as such it should be adaptable so as to satisfy the gamut of user requirements. Regardless of the different approaches that have been investigated towards achieving the above, one thing they all share in common is the process of anonymizing the search logs. User data anonymity can be achieved through many technical solutions such as *pseudo identity*, *group identity* and *encryption*. Each of the above approaches is a gradational advancement of privacy protection of the precedent. In the following paragraphs,



we outline the most widely used approaches to web data anonymization without impairing personalization.

### ***Pseudonymous Personalization***

One personalization system which allows users to remain anonymous during their personalized web browsing is the Janus Personalized Web Anonymizer [9]. Janus functions as a proxy between a user and a web site. For each user's search session, Janus automatically generates a different alias so as to establish an anonymous user account at the website. For example, user John Smith desires to navigate to the New York Times web site. Before John starts up his web browser and connect to the New York Times web site, Janus request from John to be recognized from Janus proxy and thus asks to fill a Janus authentication form. This form requires John to give a username that is recommended to be the email address and a secret- id1 and S1-. After Janus has achieved the required information about John, it allows John to navigate to the New York Times site. If John navigates for the first time to this site, in order to establish an account, sends John a registration form. John can simply fill the registration form with strings "\U" for username, "\P" for password and "\@" for e-mail address. These strings are recognized by Janus and compute aliases on John's behalf. For every site in which John navigates, different aliases are computed by Janus, which are all distinct from other users (u1, p1), (u2, p2), (u3, p3).

A similar system to Janus is Lucent Personalized Web Assistant (LPWA) [10]. LPWA is a pseudonymous tool that let Web sites offer identification based services without linking to user's actual identities.

Another approach [11] presents an architecture that allows users to create with minimal effort their personas with the aid of Persona Manager (subset of information) and through these authenticated personas provide information to service providers without revealing their identity. Service providers use these personas to enhance accuracy in personalized services. For anonymity and further privacy protection the architecture support multiple personas for each user, so as to not underline identity and not match linking personas to each user. So, when an information seeker navigates to a service provider website the communication is established between the Personal Server Device (PSD) and service provider's system. The user selects a persona to release to service provider and the service provider after authentication of the persona, begin to communicate with the user so as to provide personalized services.

### ***Distributed Personalization***

Distributed personalization has been investigated in the domain of collaborative filtering. Systems which support collaborative filtering based on the assertion that like-minded users with similar needs can be divided into groups of similar users. Consequently, personalization is done in users' group level instead of an individual user level. Search engines construct a group users profile and according to the variation of topical interests, dissimilar group of user profiles are constructed which each group profile sharing a distinct user identity [21].

An approach of privacy protection in collaborative web personalization is the meta-search engine I-Spy [22]. I-Spy relies on tracking and capturing via the click through data the user's preferences. It also relies on the *hit-matrix* so as to construct a community profile. Each individual interaction of user doesn't record and thus search history cannot be related to a particular individual user and thereby there is no concern of compromising user's privacy. Hit-matrices decay hit-values so as to keep up with the alternating preferences of community over time so as to achieve personalization while preserving anonymity of individual users. It is important to declare that different hit-matrices exist for different communities of users. A community of users is discernable from other popular and recently accessed communities. In the I-Spy start-page of a community, near the query box there is a tick-box "private" which gives the opportunity to users to exclude their search queries from being shown to other community members.

Another approach is a Firefox web browser plug-in called TrackMeNot [21] which periodically randomizes search queries to search engines. This method's goal is to make an individual's user profile to look like a group of users profile by matching firstly common queries and mix them so as to resemble that belong to a group of users and not to a certain user.

[13] implemented a system called Masks (Managing Anonymity while Sharing Knowledge to Servers). The system adapts pseudonym to group-based personalization. The system consists of a server-side, Masks server, which functions as proxy between users and web sites, and privacy and security agent (PSA) which functions as an intermediary between users and Masks server. Each user has a temporary identification that adopts while interacting with a web site and is associated with the user's interest in a thematic topic through a use of a semantic tree. For example, sites that offer travel information and the group interested in travel shares one mask, thus on one hand users can savour personalized services but on the other the system can't profile each individual user. Users can associate with a majority of groups and masks. The PSA gives the opportunity to the user to configure the masks and undertake other functionalities such as blocking and filtering privacy violations, such as cookies and web bugs.

### ***Anonymous personalization***

Anonymity means that neither a user's identity nor his location can be emanated and tracked online [5]. Thereby, construction of a user's profile can't be build even at a group level [21]. There exist anonymous networks such as the web browser Torpark, which is based on Tor onion-routing network, to obscure the communication path of users, using a network of routers that breaks the link between incoming and outgoing traffic [19]. A search engine disables to decipher where the query derives from, but the retrieved results can return to the correct user through Tor Network [21]. Tor [19] consists of over 800 routers and is at disposal to an estimated number of 200.000 users. Here, we present approaches that we pay regard to online anonymity for personalized web services.

One approach is presented in [29]. This approach is based on the assumption that a personalized query consists of two parts  $\langle d, q \rangle$ . The query  $q$  is unstructured data and contains sensitive information while  $d$  contains demographic and interests' information which is used to personalize the retrieved results. At this point, a privacy breach is discerned. A detailed navigation  $d$  may match through links and observed paths of users to a small number of users or to a unique  $q$ . To fill this void, a user pool is introduced which utilizes the semi-honest model and anonymous communication channel exists between each user and the user pool. Thereby, before the user interacts with the search engine and submits a query  $q$ , he must first register with the user pool his personal information  $d$ . The user pool presents the personal information generalized  $d'$  where  $d'$  contains less but important information, than  $d$ . For example, a user in his demographic data reveals age, gender, zip code. If  $d$  contains "Age=25", then  $d'$  after generalized personal information becomes "Age in [20,30]". Therefore, the user submits to the web service consequently  $\langle d', q \rangle$  and it is feasible to achieve personalization without privacy breach and without the user being concerned about disclosing his identify because personal information according to this approach remains anonymous.

Another approach is presented in [1]. This approach can be classified both in the case of anonymity and the encryption that we describe next, because based on two specific solutions so as to achieve balance between privacy and personalization. The first approach of anonymizing query logs is through a cryptographic technique based on secret shares. This technique relies *on-the-fly elimination* with secret sharing and consists of two primary issues. The first issue is to remove retrieved results that uniquely identify a user. But many times a specific query may prove to be not as uncommon as originally presumed and if the data is removed it is difficult to be recovered, thus meaning that valuable data can be potentially lost. The second issue is that a service provider needs to keep a histogram of sub-

mitted queries so as to achieve accuracy in the retrieved results. To fill this void, threshold cryptography or a secret sharing application has been proposed. The secret  $S$ , illustrates the query and then splits it into a number of shares. Each share is not indicative on its own, but in combination the secret can be decoded if it appears a  $t$  times before been decoded. The second solution relies on splitting personality so that a service provider can't correlate the user interests with a specific user. For example, if a user is interested in "football" and "cooking", upon personality split, the user will look like two distinct users with two separate preferences. In example of the 62 year old woman living in Georgia from AOL disclosure we mentioned in a previous section, they found that she consists of 165 different personalities. These two mechanisms contribute to anonymize the users and make them seem dissimilar so as to achieve a balance between privacy and personalization.

### ***Encryption***

Encryption is the process of transferring information -plaintext- with the aid of an algorithm -cipher- to make the plain text unreadable by anyone, except those possessing specific knowledge, usually referred to a possession of public or private key. Each key is interdependent to each other. If one key is used for encryption, the other is used for decryption. Encryption is used to protect data which is being transferred via networks [31].

One approach in this respect is introduced in [30] and it is called the de-identification approach. This approach distinguishes the data in identifiable which contains user names, account IDs, card numbers. These data can easily map users. The other classification of data is the piece of data which contains the user preferences and interests which is not as sensitive as the previous. The basic idea of the de-identification approach is to encrypt identifiable data with the domain salt and makes it infeasible to correlate users with their profiles under different sites. The remaining data which consists of preferences doesn't undergo changes so that the personalization can be achieved.

## **5. Challenges to Web Data Anonymization - Further Proposals**

Privacy in personalized web search poses many challenges that need to be addressed. In this section we outline some challenges that have been identified after applying some of the approaches previously discussed. The quest in privacy preservation for personalized applications is to ensure a balance between personal data protection and user-specific services. The design guidelines which we described above account for different levels of privacy protection with the encryption method to be at the highest level.

The first approach for safeguarding and enhancing privacy in personalized search we have addressed is the pseudo identity approach. Pseudonymous personalization enables information seekers to remain anonymous through aliases during the different user search sessions [28]. Namely, when a user reveals his IP address, the system emanates geographic information which denotes the *whois* service [21]. Furthermore, the majority of the online web sites require the user -in order to fill a registration form- to provide a valid e-mail address which has a result to reveal personal information about the user's identity. With a pseudo identity, such personal information is protected. But, the approach of pseudonymous personalization ostensibly seems to be a panacea however, actually offers the lowest level of privacy protection because if grouping a number of queries from the same user, it is possible to identify the user.

The approach of group identity denotes higher degree of privacy than the first level of pseudonymous personalization because on one hand an individual user profile cannot be constructed and on the other the identity of one user is not discernable and lost in a group identity, so it is a hard task to emanate true information of each individual user [21]. Higher privacy protection than the approach of group identity provide the anonymous personalization but some user information is kept at the search engine in order to mine search logs and thus it is possible to emanate a user's identity from distinct searches. The encryption approach offers a fully protected percentage of user's privacy but it is difficult to be achieved because the implementation of encryption and decryption is a costly procedure [21].

Achieving a substantial gain and to bridge the gap between privacy and personalization we have to overcome these challenges and define new protocols. Personalization is a promising approach but the concern of user's privacy is beyond dispute. One movement to enhance privacy is the Platform for Privacy Preferences Project (P3P), created by the Wide World Web Consortium [6]. This Platform empower websites to express their privacy policies in a standard machine-readable vocabulary so as to provide information to users about the sites' privacy policies and underlying to them when a privacy breach is exist.

Another proposal for enhancing privacy in personalized search arouse by [7] which supports that personalization gives amelioration not to the majority of retrieved results after inputting a query. So according to [25], not all searches need to be personalized. The contribution of personalization is useful when a large click entropy is discerned, meaning that various pages have been clicked for an input query, while the detection of low click entropy indicates that only a few pages have been clicked, thus there is no need to apply personalization. As a result the need to search results is mainly pronounced for informational queries and less so for navigational ones. Furthermore, according to [12] introduce manually

selection of privacy according to the users' requirements. The system offer the opportunity to users' designate the level of privacy they prefer and declare which preferences and interests desires to be *public*, *semi-public*, *private* and *don't share*. This system with the correlation of personalize only queries with large entropy, users achieve personalization and control by themselves the privacy level they prefer. Lastly, taking account the P3P Platform, users have a better image about the privacy policy that a website supports and enhance the navigation to the current website without concerns on behalf of the users for their privacy breach.

## 6. Conclusion

Personalization is a promising approach to enhance accuracy in retrieved results so as to cater for the user needs and overcome the problem of polysemy by the reason of rapidly flourishing documents that are indexed in search engine databases. The two predominant approaches towards personalization are: explicit and implicit user profiling, with the latter respecting the user interests and search preferences. The acquisition of user personal data is a considerable task and the initiatory stage in order to achieve effective personalized assistance and to avoid mismatching retrieved results. These pieces of personal data are very beneficial to capture the tastes of users and retrieve relevant results but users are concerned about their privacy breach. In this paper we have summarized the most known privacy issues in personalized web search and outlined their strengths and weaknesses in the hope of paving the ground for most advanced data protection services in the next generation search engines.

## References

- Adar E. 2007. "User 4xxxxx9: Anonymizing Query Logs". In *Query Logs Workshop, at the 16th WWW*.
- Agichtein E., Brill E., Dumais S. and Ragno R. 2006. "Learning User Interaction Models for Predicting Web Search Result Preferences". In *Proceedings of the 29th annual international ACM SIGIR conference on Research and development in information retrieval*, New York, NY, USA.
- Agichtein E., Zheng Z. 2006. "Identifying "Best Bet" Web Search Results by Mining Past User Behaviour". In *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD, New York, NY, USA.
- Aktas M., Nacar M. and Menczer F. 2004. "Personalizing PageRank Based on Domain Profiles". In *Proceedings of the sixth WEBKDD workshop, in conjunction with the 10th ACM SIGKDD conference*, Seattle, Washington, USA.

Al-Muhtadi J., Hill R. and Campbell R. 2004. "A Privacy Preserving Overlay for Active Spaces". UbiComp, Privacy Workshop, Nottingham, England.

De Grande R. and Zorzo S. 2006. "Privacy Protection Without Impairing Personalization by Using the Extended System MASKS and the Extended Contextualized P3P Privacy Policies". In *Proceedings WebMedia '06 Proceedings of the 12th Brazilian Symposium on Multimedia and the web*, ACM, New York, NY, USA.

Dou Z., Song R., and Wen J.R. 2007. "A large-scale evaluation and analysis of personalized search strategies." In *Proceedings of the 16th international conference on World Wide Web*, 581-590, ACM, New York, NY, USA.

Eirinaki M., Vazirgiannis M. and Varlamis I. 2003. "Using Site Semantics and a Taxonomy to Enhance the Web Personalization Process." In *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD, New York, NY, USA.

Gabber E., Gibbons B. P., Matias Y. and Mayer A. 1997. "How to Make Personalized Web Browsing Simple, Secure, and Anonymous". In *Financial Cryptography '97* (Vol. 1318), Berlin- Heidelberg - New York: Springer Verlag.

Gabber E., Gibbons B. P., Kristol M. D., Matias Y. and Mayer A. 1999. "Consistent, Yet Anonymous, Web Access with LPWA". In *Communications of the ACM*, Volume 42, Issue 2, New York, NY, USA.

Hitchens M., Kay J., Kummerfeld B. and Brar A. 2005. "Secure Identity Management for Pseudo-Anonymous Service Access". In *Proceedings of the Security in Pervasive Computing: Second International Conference*, Lecture Notes in Computer Science Volume 3450/2005, pp. 48-55, Boppard, Germany.

Hawkey K. and Inkpen M. K. 2006. "Examining the Content and Privacy of Web Browsing Incidental Information". In *Proceedings of the 15th international conference on World Wide Web*, ACM, New York, NY, USA.

Ishitani L., Almeida V. and Wagner M., Jr. 2003. "Masks: Bringing Anonymity and Personalization Together". *IEEE Security & Privacy Magazine*, Volume 1, Issue 3, 18-23. IEEE Educational Activities Department Piscataway, NJ, USA.

Kazunari S., Hatano K. and Yoshikawa M. 2004. "Adaptive Web Search Based on User Profile Constructed without Any Effort from Users". In *Proceedings of the 13th international conference on World Wide Web*, New York, NY, USA.

Kiraly C. 2007. "Privacy vs. Profiling on the Internet". Conference "INTER: A European Cultural Studies Conference in Sweden", organised by the Advanced Cultural Studies Institute of Sweden (AC SIS) in Norrköping.

Kobsa A. 2007. "Privacy-Enhanced Personalization". In *Communications of the ACM*, Vol. 50, Issue 8, New York, NY, USA.

Micarelli A., Gasparetti F., Sciarrone F. and Gauch S. 2007. "Personalized search on world wide web". Published in book: *The adaptive web*, Springer-Verlag, Berlin, Heidelberg, ISBN: 978-3-540-72078-2.

Pretschner A., Gauch S. 1999. "Ontology Based Personalized Search". In *Proceedings of the 11th IEEE Intl. Conf. on Tools with Artificial Intelligence*, Chicago, pp. 391-398.

Saint-Jean F., Johnson A., Boneh D. and Feigenbaum J. 2007. "Private Web Search". In *Proceedings of the ACM workshop on Privacy in electronic society*. New York, NY, USA.

Semeraro G., Degemmis M., Lops P., Thiel U. and L' Abbate M. 2003. "A personalized information search process based on dialoguing agents and user profiling". In *Proceedings of 25th European Conference on IR Research, ECIR*, Lecture Notes in Computer Science, Volume 2633/2003, 548.,Pisa, Italy

Shen X., Tan B. and Zhai C. 2007. "Privacy Protection in Personalized Search". *ACM SIGIR Forum*, Volume 41 Issue 1, New York, USA.

Smyth B. and Balfe E. 2006. "Anonymous personalization in collaborative web search". *Information Retrieval*, Springer Link, Vol. 9, No 2, 165-190.

Sugiyama K., Hatano K. and Yoshikawa M. 2004. "Adaptive Web Search Based on User Profile Constructed without Any Effort from Users". In *Proceedings of the 13th international conference on World Wide Web*, New York, USA.

Tanudjaja F. and Mui L. 2002. "Persona: A Contextualized and Personalized Web Search". In *Proceedings of 35th Annual Hawaii International Conference on System Sciences (HICSS'02)*-Volume 3, Big Island, Hawaii, p. 67.

Teevan J., Dumais S. and Liebling D. 2008. "To personalize or Not to Personalize: Modeling Queries with Variation in User Intent". In *Proceedings of the 31st annual international ACM SIGIR conference on Research and development in information retrieval*, New York, NY, USA.

Teltzrow M. and Kobsa A. 2004. "Impacts of user privacy preferences on personalized systems". *Designing Personalized User Experiences in eCommerce*, Human-Computer Interaction Series, Springer Link, Volume 5, Section 5, 315-332.

Tene O. 2008. "What Google Knows: Privacy and Internet Search Engines".



<http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=omertene&sei-redirect=1#search=What+Google+Knows:+Privacy+and+Internet+Search+Engines>

Wang Y. and Kobsa A. 2008. "Technical Solutions for Privacy-Enhanced Personalization". In Mourlas, C. and Germanakos, P. (Eds.), *Intelligent User Interfaces: Adaptation and Personalization Systems and Technologies*. PA: IGI Global, Hershey.

Xu Y., Wang K., Yang G and Fu W.C. A. 2009. "Online Anonymity for Personalized Web Services". In *Proceedings of the 18th ACM conference on Information and knowledge management*, New York, NY, USA.

Zheng J., Yao J. and Niu J. 2008. "Web User De-Identification in Personalization". In *Proceedings of the 17th international conference on World Wide Web*, New York, NY, USA.

<http://en.wikipedia.org/wiki/Encryption>

# Knowledge as a public or private good? A new twist to an old tale

## A comparative human rights analysis of the protection of knowledge creation and diffusion

---

---

Katarzyna Gracz

---

---

### 1. Introduction

The disagreement on the nature of knowledge and, consequently, on the most just and efficient model of protecting its creation and dissemination can be traced back to the theories explaining the *raison d' être* of copyright. The Lockean labour-desert concept treats products of mind on a par with the fruits of physical labour as the creator's private property. It recognises the natural property right that authors acquire in their work by mixing their labour with the material object, through which their idea is expressed.<sup>1</sup> By contrast, Kant's theory differentiates between the external things that could be owned or disposed of, which are regulated by the rules of private property, and the intellectual works perceived as "continuing expression of [the creator's] inner self"<sup>2</sup>, that constitute an inherent part of the author's personality and therefore are regulated by personal rather than patrimonial rights (e.g. property rights).<sup>3</sup> In addition to the author's rights, the Kantian approach recognises certain rights of the public to access intellectual creations, therefore it perceives knowledge as exhibiting characteristics of public goods.<sup>4</sup> The middle-ground is represented by the Hegelian theory which, despite regarding creative ability as an inalienable part of the self, treats expression of the intellectual work in an external medium as an alienable good, thus capable of being the subject of private property.<sup>5</sup>

---

1. This approach is reflected e.g. in the American system of copyright which is based on the principle of the unlimited alienability of copyrights. See Natanel Neil (1994), *Alienability Restrictions and the Enhancement of Author Autonomy in United States and Continental Copyright Law*, 12 Cardozo Arts & Ent LJ 1.

2. Ibidem, p. 7.

3. This approach, called monist, is illustrated e.g. by the German copyright law, that treats authors' rights as unitary, personal and inalienable. See Ibidem, pp. 7-8.

4. Ibidem, p. 7.

5. This attitude is present in the dualistic theory of copyright which assumes that the author's personal and economic interests are each protected by a legally and conceptually distinct set of rights, represented e.g. in the French copyright law. See Ibidem, pp. 8-9.

This polemic as to the nature of knowledge goods has always been present in the doctrine of intellectual property law. Nowadays, it still divides academics, policy-makers and judges. Obviously, the discussion is most vivid and aggressive between the right- and stake-holders using their argumentation to support lobbying and litigation. The proponents of the knowledge-as-private-property approach argue that it offers the only efficient mechanism to encourage creation and innovation and they employ the rhetoric of *free riding* and *theft* to discourage unauthorised use. In response to this, those in favour of the knowledge-as-a-global-public-good approach, have developed an abundant critique, supported by various arguments comprising *inter alia* philosophical and economic analyses.

This paper proposes a distinct perspective on this problem by using the concepts that have already been elaborated on and placing them in a new comparative scheme. It will show that it is possible to reconstruct the discourse on the nature of knowledge goods in the domain of human rights law, where the same two divergent stances have been taken<sup>6</sup>. At one extreme lies the approach represented in the Universal Declaration of Human Rights and the International Covenant on Economic, Social and Cultural Rights, which recognises the *global-public-good* nature of knowledge and focuses on providing safeguards for the general public's access. At the other extreme lies the case law of the European Court of Human Rights as well as the regulations of the Charter of Fundamental Rights of the European Union that seem to approach knowledge as a private or at least a club good. This analysis will attempt to prove that, although primarily these two perspectives seem to be contradicting, at least in the human rights domain, they might be reconciled through a proper adjudication process based on the social function of the right to property.

## 2. Knowledge as a global public good?<sup>7</sup>

### 2.1 Article 27 of the Universal Declaration of Human Rights

For decades human rights<sup>8</sup> law and intellectual property rights<sup>9</sup> law have developed in "*splendid isolation*" from one another, notwithstanding the fact that the found-

---

6. In this paper I will approach human rights from the positivist perspective i.e. as recognised in the international human rights documents, rather than from the naturalist paradigm which claims that human rights should be primarily seen as ethical demands. Moreover, I will limit my analysis solely to the instruments of international human rights law applicable to the European region.

7. For the very well developed theory of knowledge as a global public good as enshrined in the UDHR and the ICESCR, by which this chapter is mostly inspired see Shaver L.B. (2010) *The Right to Science and Culture*, Wisconsin Law Review.

8. Hereinafter HR's.

9. Hereinafter IPR's.

ing document of human rights law – the Universal Declaration of Human Rights<sup>10</sup> – expressed the first attempt to protect creation and diffusion of knowledge.

The issue of the protection of interests in intellectual creations is dealt with in the Universal Declaration in Article 27, which reads as follows:

1. Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.
2. Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

The dualistic construction of this provision indicates that the drafters of the Universal Declaration perceived human creativity from two different perspectives: as a right of the public to access the results of artistic and scientific works and as a right of creators to have the moral and material rights in their works protected. The structure of Article 27 also contains the assumption that the right of creative individuals, as regulated in the second paragraph, should be subordinate to the right of whole humankind to enjoy the results of all the intellectual work of others, which is enshrined in the first paragraph. The same interpretation may also be derived from the drafting history.

### 2.1.1 Historical Context of the Drafting Process

#### *a) Preventing future misuse of science and abuse of scientists' work*

The most important historical factor triggering the drafting process and shaping the negotiations of the Universal Declaration of Human Rights was the experience of World War II. The acts of aggression against human dignity committed during that global conflict constituted the actual reason for the states to draft a document which would assure that the “*disregard and contempt for human rights [that] have resulted in barbarous acts which have outraged the conscience of mankind*”<sup>11</sup> would never be repeated. Although never mentioned explicitly in the document, World War II and the Holocaust clearly motivated the framers of the Declaration.<sup>12</sup> Thus, Article 27 should primarily be regarded as a reaction to the massacres led by the Nazis and Stalin, which were committed with the wide instru-

---

10. Universal Declaration of Human Rights, GA Resolution 217 A (III), UN Doc. A/810 (1948) [hereinafter UDHR or the Declaration].

11. Preamble of the UDHR.

12. For detailed history of the UDHR's drafting process, see e.g. Glendon M. A. (2001), *A World Made New: Eleanor Roosevelt and the Universal Declaration of Human Right*, Random House;

mental usage of science and technology<sup>13</sup>. During these through the acts of the scientists and engineers conscripted and forced to work without remuneration by the totalitarian regimes, which were “*seeking to exploit the applications of science for purposes of power aggrandisement*”<sup>14</sup>. The content of this article was to a large extent shaped by the post-war public debates, attracting active participation of many eminent scientists<sup>15</sup>, who highlighted the urgent need to protect science and technology from misuse in the future.<sup>16</sup>

According to the drafters, the recognition of the right to a just remuneration of intellectual creators and the right of every individual to enjoy the benefits of scientific and technological development was the best legal instrument to avoid the future misuse of science in a way contrary to human dignity,<sup>17</sup> and so this should be perceived as the primary aim of Article 27 of the Universal Declaration.

#### *b) Expanding access to science and culture*

In the years preceding the negotiations of the Universal Declaration, scientific and artistic activities were highly elitist in nature<sup>18</sup>. As was the access to their

---

Morsink J. (1999), *The Universal Declaration of Human Rights: Origins, Drafting and Intent*, University of Pennsylvania Press.

13. Proctor R. N., *Nazi Doctors, Racial Medicine, and Human Experimentation*, in Annas G.J., and Grodin A. M. (eds.) (1992), *The Nazi Doctors and the Nuremberg Code, Human Rights in Human Experimentation*, Oxford University Press; Josephson P. R., (2005) *Totalitarian Science and Technology*, Prometheus Books.
14. Claude R. P., *Scientists' Rights and the Human Right to the Benefits of Science* in Chapman A.R., and Russel S. (eds.) (2002), *Core Obligations: Building a Framework for Economic, Social and Cultural Rights*, Intersentia, p. 249.
15. Among the strong supporters of the Declaration to protect the science and technology from misuse were inter alios: Julian Huxley, the British biologist and writer who served as the first director of UNESCO, W.A. Noyes, the American chemist and J.M. Burgers a member of the Netherlands Academy of Science, See Chapman A.R., (2009), *Towards an Understanding of the Right to Enjoy the Benefits of Scientific Progress and Its Applications*, *Journal of Human Rights*, 8:1, 1-36, p. 5.
16. Ibidem.
17. “[A]t the signing of the Universal Declaration, the United Nations had come to envision the sharing of scientific and cultural knowledge as something that could unite an international community; a common task that would contribute to cross-cultural understanding and yield a more secure world than that which characterised the 1930s and early 1940s.” Shaver, (2010), p. 25.
18. See e.g. Chapman A.R., (1998) *A Human Rights Perspective on Intellectual Property, Scientific Progress, And Access to the Benefits of Science*, Panel Discussion to Commemorate the 50th

fruit<sup>19</sup>. It was only after the end of World War II that higher education was opened to the masses and the artistic creations of various peoples started to be widely appreciated on par with the so called *high culture*, thanks to an awakening of the interest in traditional folk culture.<sup>20</sup> It was exactly at the time when the Universal Declaration was being drafted that the democratisation of both science and culture started. This process was universal around the globe.

In the United States, as noted by Lea Shaver “[t]he Roosevelt Administration explicitly called on science to solve pressing human challenges and serve the nation’s collective war effort. After the war in particular, a new enthusiasm emerged within the scientific and academic community to put its efforts at the service of the humanity.”<sup>21</sup> The economic programmes of the New Deal provided public funding for the diffusion of science and culture inter alia by financing public libraries and theatres.<sup>22</sup> They were also highly sympathetic to the growing interest in folk art and oral history<sup>23</sup> that gave the floor to so-far unheard, often marginalised social groups such as peasants, racial minorities, immigrants, women etc.

Similar democratisation processes, although in different circumstances, were also present in the post-colonial world<sup>24</sup>, where the recent collapse of empires completely changed the scientific and cultural arena by allowing native languages and cultural heritage to enter the scene.

An analogous situation was observed in the communist countries, where it fitted perfectly with the general ideology of empowering the masses at the expense of the hitherto privileged social elites. The democratisation of science and culture in the countries behind the Iron Curtain was epitomised by the public funding for libraries, cinemas, theatres and so-called *houses of culture*, with the largest of them, called “*palaces of culture and science*”, offering the possibility the masses to participate in the scientific and cultural life of the community. In socialist countries, the post-war enthusiasm mixed with the novel slogans of the as yet not fully discredited communistic ideology created massive popular movements for the benefit of science and culture. The democratisation of science also took

---

Anniversary of the Universal Declaration of Human Rights, WIPO, Geneva, November 9, 1998, p. 7.

19. See: Shaver, (2010), p. 5; Shaver L.B., and Sganga C., (2009), *The Right to Take Part in Cultural Life: On Copyright and Cultural Rights*, Wisconsin International Law Journal, Vol. 27, p. 637.

20. Ibidem, p. 23.

21. Ibidem, p. 43.

22. Ibidem, p. 23.

23. Ibidem.

24. Ibidem, p. 25.

the form of empowering young people from the lower classes, especially from workers' and farmers' families, through special quotas assuring their presence at the universities. The democratisation of culture in this region was also exemplified by multiple artistic initiatives in the public sphere (the aesthetic value of which is nowadays widely questioned), such as the huge paintings on the walls of buildings illustrating communist slogans, sculptures and monuments praising the communist regime etc. Very specific for this region was also the introduction of scenes from the life of the so-called *simple people*, such as farmers and workers, as themes in artistic works in all genres of art.

As the above examples illustrate, the democratisation of science and culture at this time proceeded in two directions. The first was focused on enabling active participation in artistic and scientific life to the wide masses (university quotas, support for folk culture). The second was providing the general public with the right to benefit from the artistic and scientific work of others (public funding for libraries and theatres). Although it may seem that scientific and cultural development is an independent natural phenomenon, scientific discovery, the introduction of a new technology or the creation of an artistic work *per se* do not necessarily entail general access to such developments. At the time when the Universal Declaration was born, the widespread access to art and the benefits of scientific development were far from obvious.<sup>25</sup>

The willingness to democratise science and culture should therefore be perceived as another crucial factor shaping the wording of Article 27 of the Universal Declaration.

### 2.1.2 Drafting History

The historical context in which the negotiations of the Universal Declaration took place sheds important light on the aims guiding the drafters when incorporating Article 27. This understanding would however be incomplete without a closer analysis of the document's drafting process itself.

The dualistic construction of Article 27, as mentioned above, indicates that the drafters approached human creativity from two different perspectives: as a right of the public to access the results of artistic and scientific works, and as a right

---

25. See the examples of the electrification process in the United States and the discovery of the polio vaccine as described in depth by Lea Shaver, stating that, at the time when the Universal Declaration was being drafted the enormous and outstanding effort of the massive popular movements was necessary for both assisting the discovery of new technologies in the spheres neglected by the mainstream science and diffusing the existing ones for the benefit of the general public in: Shaver, (2010), pp. 26-27.

of creators to have the moral and material rights in their works protected<sup>26</sup>. The most important fact, essential for the proper interpretation of this provision, is that these two perspectives, represented in the document by two separate paragraphs, triggered completely different reactions amongst the drafters and, consequently, followed divergent histories.<sup>27</sup>

The right to enjoy the benefits of scientific and artistic advances as regulated in the first paragraph of Article 27 UDHR did not create much controversy for it was supported by all the delegates favouring the aforementioned arguments of the democratisation of science and culture as well as the prevention of future misuses contrary to human dignity. The drafters shared a common sentiment *“that even if all persons could not play an equal part in scientific [and artistic] progress, they should indisputably be able to participate in the benefits derived from it”*<sup>28</sup>, as was aptly stated by the French delegate René Cassin.

By contrast, the creators’ rights, as expressed in what became the second paragraph of Article 27, triggered a hot debate.<sup>29</sup> The French proposal to include the protection of moral and material interests of authors in the Declaration raised multiple objections from other drafters, who either regarded the rights of authors as lacking sufficient importance to be given the status of a basic human right<sup>30</sup> or thought

26. As it was argued by the Chinese delegate calling for inclusion into the provision of the additional phrase “share in benefits”: *“in the arts, letters and sciences alike, aesthetic enjoyment has two sides: a purely passive aspect when one appreciates beauty and an active aspect when one creates it.”* See Claude, p. 253.

27. Moreover the first draft of the Declaration prepared by the director of the Division on Human Rights at the United Nations, John Humprey, did not include the right to the protection of interests in intellectual creations and it only referred to “the right to participate in the cultural life of the community, to enjoy the arts and to share in the benefits of science” which eventually was transformed into what became Article 27(1) of the UDHR. The protection of the rights of the creators was added only at the later stage by the French delegate René Cassin, who introduced a new provision which initially stated that “[t]he authors of all artistic, literary, scientific works and inventors shall retain, in addition to just remuneration for their labour, a moral right on their work and/or discovery which shall not disappear, even after such a work or discovery shall have become the common property of mankind.” See: Yu P. K, (2007), *Reconceptualizing Intellectual Property Interests in a Human Rights Framework*, 40 U.C. Davis L. Rev. 1039, pp. 1051-1052.

28. Morsink (1999), p. 219.

29. Green M., (2000), *Drafting History of Article 15 (1) (1)(c) of the International Covenant*, E/C.12/2000/15, para. 5. Online at: [http://www.unhchr.ch/tbs/doc.nsf/0/872a8f7775c9823cc1256999005c3088/\\$FILE/G0044899.pdf](http://www.unhchr.ch/tbs/doc.nsf/0/872a8f7775c9823cc1256999005c3088/$FILE/G0044899.pdf)/accessed 28.02.2011.

30. Morsink, (1999) p. 221, (where he quotes Corbet, the delegate from the United Kingdom saying that copyright “was not a basic human right” and the Australian representative claiming that “the



those rights had already been adequately covered by the provision protecting the right to property<sup>31</sup> and other international regulations outside human rights law,<sup>32</sup> it was even claimed that special protection for intellectual property would entail an elitist perspective<sup>33</sup> in the otherwise egalitarian document, that was supposed to implement the concept of universal human rights. The second paragraph of Article 27 was repeatedly rejected and even after its eventual passing, it failed to be regarded by the drafters as a pure right of creative individuals, and was more perceived as an additional element of protecting the public, an attitude strengthened by the increasingly voiced arguments that *the moral rights* part of the regulation should also strive to ensure universal access to works in their original form<sup>34</sup>.

The strong opposition to the second paragraph of Article 27 UDHR<sup>35</sup> expressed throughout the whole negotiating process was not moderated even at the final stage; hence the eventual adoption of this provision was hardly articulation of the consensus, with merely 18 votes in favour as opposed to 13 votes cast against, and 10 abstentions.<sup>36</sup>

What follows from the structural logics of Article 27, as well as the historical interpretation of this provision, is that the human rights' protection of interests in intellectual creations expressed in the UDHR seems focused mostly on providing universal access to the results of human creativity. The protection of the rights of individual creators was treated as instrumental and subservient to the needs of the general public. The drafters not only failed to recognise the results of intel-

---

indisputable rights of the intellectual worker could not appear beside fundamental rights of a more general nature, such as freedom of thought, religious freedom or the right to work".)

31. Ibidem.

32. Ibidem, (recalling Corbet's statement that "copyright was dealt with by special legislation and in international conventions".)

33. Official Records of the Third Session of the General Assembly, Part I, Social and Humanitarian and Cultural Questions Third Committee, Summary of Records of Meetings, 21 September to 8 December 1948, pp. 619–34 Quoted after: Chapman A.R., (2001), *Approaching Intellectual Property as a Human Right*, Copyright Bulletin, volume XXXV, no. 3, p. 11.

34. Morsink, (1999), p. 221, quoting the Chinese delegate, Chang, arguing that "the purpose of the joint amendment was not merely to protect creative artists but to safeguard the interests of everyone". For that reason "literary, artistic and scientific works should be made accessible to the people directly in their original form. This could only be done if the moral rights of the creative artists were protected."

35. Such a strong opposition as that expressed against provisions on the protection of interests in intellectual creations was unique in the whole drafting history of the Universal Declaration. See: Shaver, (2010).

36. Morsink, (1999), p. 222.

lectual work as the exclusive property of their creators, but also whilst perceiving it as necessary to maintain a proper balance between the rights of individual authors and inventors on the one hand, and the public on the other, they attached paramount importance to the general welfare.

## ***2.2 Article 15 (1) of the International Covenant on Economic, Social and Cultural Rights***

The same attitude was expressed in the International Covenant on Economic, Social and Cultural Rights<sup>37</sup>, which was introduced, together with the International Covenant on Civil and Political Rights, to give force to the unenforceable political declarations expressed in the UDHR. At no stage of the drafting process of the two Covenants did an automatic inclusion of the compromises previously achieved in the Universal Declaration take place<sup>38</sup>. However, Article 15 (1) (1) of the ICESCR, which is devoted to the protection of interests in intellectual creations, closely resembles Article 27 of the UDHR, as does the history of its drafting.

Article 15 (1)(1) of the ICESCR reads as follows:

1. The States Parties to the present Covenant recognise the right of everyone:
  - a) To take part in cultural life;
  - b) To enjoy the benefits of scientific progress and its applications;
  - c) To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

### **2.2.1 Drafting History**

Article 15 (1)(1) of the ICESCR, like Article 27 of the UDHR, consists of the same three components dealing with the right to culture, right to scientific advancement and protection of rights in intellectual creations. Similar to the drafting history of Article 27 UDHR, there was a strong support from all representatives throughout the negotiations for the right of everyone to share in the benefits of science and to participate in the cultural life of the community, viewed as “the determining factor for the exercise by mankind as a whole of many other rights”<sup>39</sup>. However, the rights of authors and inventors did once again trigger a heated debate.<sup>40</sup> The strongest

37. International Covenant on Economic, Social and Cultural Rights G.A. res. 2200A (XXI), 21 U.N.GAOR Supp. (No. 16) at 49, U.N. Doc. A/6316 (1966), 993 U.N.T.S. 3, entered into force 3 January 1976, (hereinafter ICESCR or the Covenant).

38. See e.g. Yu, (2009), p. 1060; Green (2000), paragraph 18.

39. Statement by the representative of UNESCO Havet, cited after Green (2000), para 20.

40. Ibidem.

objections to incorporating those rights were raised by the Soviet Union together with the whole Eastern bloc, which argued that the people's right to benefit from science and culture should not be intermingled with property rights. The opposition subsided only after assurances that the rights of intellectual creators were not equal to the right to private property and their primary purpose was to prevent others from altering the original expression of intellectual and artistic creations and that they should be regarded as essential preconditions for cultural and scientific freedom and wide public participation in scientific and cultural life.<sup>41</sup>

Hence, similar to the case of to Article 27 UDHR, the provision concerning the rights of individual creators was finally accepted only because its initial critics were eventually convinced that it should be perceived as crucial for safeguarding the interests of the community as a whole. Once again, it was claimed that the protection of authors' rights was vital for assuring public access to the authentic works<sup>42</sup>, and furthermore that it was critical to "give effective encouragement to the development of culture"<sup>43</sup>.

The drafting history of the ICESCR proves, exactly like the UDHR's, that the provision on authors' rights was eventually included only because of its instrumental character in meeting the needs of the community as a whole, which were perceived as having a stronger moral justification than the privileges of individual creators<sup>44</sup>. Hence, the three elements comprising Article 15 (1) (1) of the ICESCR must be seen as intrinsically interrelated<sup>45</sup> and therefore the protection of the results of human creativity as provided by the ICESCR cannot be viewed as constituting the monopoly property rights of creators and inventors but primarily as safeguarding access to scientific and artistic developments.

The drafters of the Covenant seemed to have been thinking of authors exclusively as individuals and did not mean to protect the interests in intellectual creations

---

41. Chapman A.R., (2009), p. 6; Chapman A. R., *Core Obligations Related to ICESCR Article 15 (1) (1) (c)*, Chapman A. R. and Sage R. (eds.), (2002), pp. 305-331 and pp. 312-316.

42. Official Records, United Nations General Assembly, Agenda item 33, 789<sup>th</sup> meeting, 1 November 1957, para. 32, p. 183.

43. Statement by the Israeli delegate. See: *Official Records*, United Nations General Assembly, Agenda item 33, 789<sup>th</sup> meeting, 1 November 1957, para. 32, p. 183.

44. *Ibidem*.

45. Committee on Economic, Social and Cultural Rights, General Comment No.17 (2005), The right of everyone to benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he or she is the author (Article 15 (1), paragraph 1 (c), of the Covenant), 12 January 2006, E/C.12/GC/17, par. 4. [Hereinafter General Comment No.17].

of legal entities.<sup>46</sup> Such an understanding of Article 15 (1) has recently been confirmed by the Committee on Economic, Social and Cultural Rights in the General Comment No.17 to Article 15 (1)(c) of the ICESCR which states that corporate entities are not protected at the human rights as they remain outside the safeguards of human rights system<sup>47</sup>.

The interpretation of both Article 27 of the Universal Declaration and Article 15 (1) of the Covenant seems to prove that, to the extent they approached the wide public access to the benefits of artistic and scientific development as universal human right superior to the rights of individual creators to have their interests in intellectual creations protected, the drafters of these documents anticipated the vision of knowledge as a global public good<sup>48</sup>, which was later developed and analysed in depth by both economists and lawyers.

### 2.3 What are global public goods?

The concept of *public goods* is traceable back to the 18th century, when David Hume discussed the difficulties inherent in providing for the common good in his "*Treaties of Human Nature*", first published in 1739.<sup>49</sup> Since then, the literature on the topic flourished. Nevertheless, it was only in the second half of the 20th century that economic, and subsequently legal, scholars started to recognise knowledge firstly as a particularly valuable resource, capable of improving the welfare of humankind<sup>50</sup>, then as also having the qualities of a public good<sup>51</sup> is only very recently that knowledge has been as being a global public good<sup>52</sup>. What, then, the features of the global public goods that are also borne by knowledge and which were foreseen by the foundational documents of universal human rights law?

---

46. M. Green (2000), para. 45.

47. *General Comment No. 17*, para. 7.

48. Shaver (2010) p. 36.

49. Kaul I., Grunberg I. and Stern M. A., *Defining Global Public Goods*, in: Kaul I., Grunberg I. and Stern M. A., (eds.) (1999) *Global Public Goods. International Cooperation in the 21<sup>st</sup> Century*, The United Nations Development Programme, Oxford University Press, p. 3.

50. See e.g. Abramowitz M., (1956), *Resource and Output Trends in the United States Since 1870*, 46 *American Econ. Rev.* 5; Solow R. M., (1957), *Technical Change and the Aggregate Production Function*, 39 *Rev. of Econ.&Statistics* 312, quoted after Shaver, (2010), p. 43.

51. See e.g. Boyle J., (1997) *Shamans, Software and Spleens: Law and the Construction of the Information Society*, Harvard University Press.

52. See e.g.: Barrett S., (2007) *Why Cooperate? The incentive to Supply Global Public Goods*. Oxford University Press, p. 45; Stiglitz J. E., *Knowledge as a Global Public Good*, in Inge Kaul, Isabelle Grunberg, Marc A. Stern (eds.) (1999), *Global Public Goods: International Cooperation in the 21<sup>st</sup> Century*.

Ideal public goods, so-called *pure public goods*<sup>53</sup>, have two main qualities: their benefits are non-rivalrous in consumption and non-excludable. The non-rivalrous nature of the good means that the consumption of its benefits by one individual does not reduce the availability of the good for the consumption of others. The non-excludability, on the other hand, means that no one can be effectively excluded from using the good. Some scholars claim that public goods “*can be thought of as special cases of externalities*”<sup>54</sup> in that they have an advantageous (in case of *public goods* or detrimental in case of *public bads*) impact on a party that is not directly involved in the transaction.

Private goods, on the contrary, are excludable and rivalrous in consumption. The buyer gains access to private goods in exchange for the price set by the market. The price mechanism allows the reaching of a state of maximum efficiency in which resources are used in the most productive way. Access to the good is conditional on the payment of its price and cannot be enjoyed by those who fail to pay the price (excludability); at the same time the consumption by one individual reduces the availability of the good for the consumption by others (rivalrousness).

Few goods are purely public or purely private - most exhibit mixed characteristics. Goods that only partly meet either one or both criteria are called *impure public goods*,<sup>55</sup> and could be divided into two categories: *club goods*, i.e. goods that are non-rivalrous in consumption but excludable;<sup>56</sup> and *common pool resources*, i.e. goods that are mostly non-excludable but rivalrous in consumption<sup>57</sup>.

TABLE No 1.

	RIVALROUS	NONRIVALROUS
EXCLUDABLE	Private goods	<i>Club goods</i>
NONEXCLUDABLE	<i>Common Pool Resource</i>	<i>Pure public goods</i>

Note: Public goods in italics, impure public goods underlined;  
[Source: Kaul I., Grunberg I. and Stern M. A., (eds.) (1999), p. 5.]

53. Kaul I., Grunberg I. and Stern M. A., (eds.) (1999), p. 3.

54. See Cornes R., and Sandler T., (1996), *The Theory of Externalities, Public Goods, and Club Goods*, 2<sup>nd</sup> ed. Cambridge University Press, p. 6.

55. Due to the scarcity of ideal public goods also the impure public goods are referred to as public goods, and the pure public and pure private goods should be approached merely as the extremes of the same theoretical public-private continuum.

56. See: Cornes R., and Sandler T. (1996).

57. See e.g.: Hardin G., (1968), *The Tragedy of the Commons*, Science 162: 1243-48; Wijkman P. M. (1982), *Managing the Global Commons*, International Organisation 36(3):511-35; Stone Ch., (1993), *The Gnat Is Older than Man: Global Environment and the Human Agenda*, Princeton University Press.

Global public goods are those public goods, the benefits of which can be enjoyed by the global *publicum*, i.e. that are not limited to any specific population defined by geography, socio-economic status or generation.<sup>58</sup> This multidimensional attitude towards the *globality* of some public goods emphasises the fact that they benefit all of humanity, notwithstanding the nationality, age, sex or socio-economic status of the person etc.,<sup>59</sup> in which they resemble universal human rights.<sup>60</sup>

Knowledge has recently been identified by economists as one of the global public goods<sup>61</sup>, since due to its non-rivalrousness, non-excludability and universal worth it can benefit simultaneously all of humankind. Moreover, according to network externalities, the value of knowledge increases in the process of sharing: ideas may become more valuable to the society as a whole if they are used to the largest possible extent<sup>62</sup>.

The non-rivalrous and non-excludable of the fruit of the human mind, however, were much earlier perfectly described by the first U.S. Patent Commissioner, Thomas Jefferson, who aptly stated:

“If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea, which individual may exclusively possess as long as he keeps it to himself; but the moment it is divulged, it forces itself into the possession of everyone, and the receiver cannot dispossess himself of it. Its peculiar character, too, is that no one possesses the less, because every other possesses the whole of it. He who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine, receives light without darkening me.

That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space, without lessening their density in any point, and

---

58. Kaul I., Grunberg I. and Stern M. A., (eds.) (1999), pp. 9-14.

59. Ibidem.

60. This multidimensional approach could be opposed to one-dimension approach that distinguishes only between “global” and “local” public goods in terms of geographical limits.

61. Other global public goods being e.g. international economic stability, international security (political stability/international peace), international environment and international humanitarian assistance. See: Joseph E. Stiglitz J.E., *Knowledge as a Global Public Good*, in Kaul I., Grunberg I. and Stern M. A., (eds.) (1999), p. 310.

62. Cornides J., (2004), *Human Rights and Intellectual Property. Conflict or Convergence*, The Journal of World Intellectual Property, 7(2), p. 136.

like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation.

Inventions then cannot, in nature, be a subject of property.”<sup>63</sup>

The globality of most knowledge should also be beyond any doubt as “a mathematical theorem is as true in Russia as it is in the United States, in Africa as it is in Australia”<sup>64</sup>.

The vision of knowledge present in Article 27 UDHR and Article 15 (1) ICESCR alike recognises its *pure global public good* attributes. Any regulations extending the rights of individual creators beyond what is provided for by the human right to the protection of interests in intellectual creations are contrary to the aforementioned provisions insofar as they change the nature of knowledge into a *club good*, which not everyone is entitled to access, or even into a *private good*, of which not only excludability but also scarcity is artificially created by legal regulations<sup>65</sup>. To be in line with the human rights’ provisions of Article 27 UDHR and Article 15 (1) ICESCR on the access to knowledge, all instantiations of the protection of individual authors must respect the vision of knowledge as characterised by its pure global public good attributes, meaning that its benefits in form of the artistic, scientific and technological advances can be shared by all humanity regardless of race, sex, age, socio-economic situation, etc.

## 4. Knowledge as a private good?

### 4.1 Case law of the European Court of Human Rights

The recent case law of the European Court of Human Rights adopted divergent attitude towards protection of knowledge creation and diffusion. The European Convention for the Protection of Human Rights and Fundamental Freedoms<sup>66</sup>,

---

63. Thomas Jefferson in his letter to Isaac McPherson, of 13 August 1813, cited after: J. Cornides, (2004), p. 149.

64. Stiglitz J.E. (1999), p. 310. Of course there are some kinds of knowledge that are of value only locally for populations defined by the geography, age or socio-economic status, but it still does not change its global public good nature as it could still be enjoyed by all the humanity without exclusion at the same time, just that not all the people would have the same interest in it. Moreover, most of knowledge, especially scientific truths are universal in nature.

65. Marlin-Bennet R., (2004), *Knowledge Power. Intellectual Property, Information and Privacy*, Boulder: Lynne Rienner Publishers, p. 13.

66. European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, 213 U.N.T.S. 222 (hereinafter the European Convention, the European Convention on Human Rights or ECHR).

contrary to the Universal Declaration of Human Rights and the International Covenant on Economic, Social and Cultural Rights, does not include separate provisions on the access to knowledge and protection of interests in intellectual creations. Moreover, until the early 1990s intellectual property right holders did not claim violations of their rights based on the European Convention, and when they eventually commenced, until recently the European Commission and the European Court of Human Rights have repeatedly refused to adjudicate directly on the protection of interests in intellectual and artistic works. It was not until the 1990s<sup>67</sup> that the European Commission finally held that Article 1 of the Protocol No. 1 to the European Convention applies to intellectual property, which was confirmed as late as 2005<sup>68</sup> by the rulings of the European Court of Human Rights.

Article 1 of Protocol No. 1 to the European Convention that was successfully invoked by the intellectual property right holders reads as follows:

Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.

The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.

The question of the protection of intellectual property was firstly assessed by the European Commission which consistently held in its three decisions dating back to the 1990s that patents [*Smith Kline & French Lab. Ltd. v. Netherlands* (1990) and *Lenzig AG v. United Kingdom* (1998)] and copyrights [*Aral v. Turkey*, (1998)] fall within the subject matter scope of Article 1 of the Protocol 1 to the European

---

67. *Lenzig AG v. United Kingdom*, App. No. 38817/97, 94-A Eur.Comm'n H.R. Dec.& Rep. 136 (1998) (patent); *Aral v. Turkey*, App. No. 24563/94 (1998) (admissibility decision) (copyright); *Smith Kline & French Lab. Ltd. v. Netherlands*, App. No. 12633/87,66 Eur. Comm'n H.R. Dec. & Rep. 70,79 (1990) (admissibility decision) (patent).

68. *Dima v. Romania*, App. No.58472/00, para.87 (admissibility decision) (copyrighted works protected by Art.1); *Anheuser-Busch Inc. v. Portugal*, App. No.73049/01, Eur. H.R. Rep. 42 [846],855-856 (Chamber 2007) (judgment of 11 October 2005) (registered trademarks protected by Art.1); *Melnychuk vs. Ukraine*, App.No. 28743/03, para.8 (admissibility decision)(2005) (intellectual property protected by Art.1 ). Cited after Helfer L.R., *Intellectual Property and the European Court of Human Rights* in: Torremans P. L.C. (Ed.) (2008), *Intellectual Property and Human Rights. Enhanced Edition of Copyright and Human Rights*, Wolters Kluwer, p. 27.



Convention. The same line of reasoning was applied by the European Court of Human Rights.

The question of the protection of copyrighted works under the European system of human rights was dealt with directly by the European Court of Human Rights for the first time in *Dima v. Romania* (2005)<sup>69</sup>. Even though the ECHR did not decide whether, under the circumstances of the case the claimant indeed had possession as the author of the graphic design, it did state that Article 1 of Protocol No. 1 to the European Convention for the Protection of Human Rights and Fundamental Freedoms protects copyrighted works. A similar logic was applied to the issue of trademarks in *Anheuser-Busch Inc. v. Portugal*<sup>70</sup>, where the ECHR held that both registered trademarks and sole applications for having a trademark registered amount to *possessions* as covered by Article 1 of Protocol No. 1. Finally, in *Melnychuk vs. Ukraine* (2005) the Court held that intellectual property in general is protected by Article 1 of Protocol No. 1 to the European Convention of Human Rights.

#### 4.1.1 Intellectual Property equated with other possessions?

As the examples above illustrate, under the case law of both the European Commission of Human Rights and the European Court of Human Rights intellectual property is protected by the European Convention's right to property. This reasoning is in line with the earlier decisions of the ECHR, which have repeatedly been giving a wide interpretation to the scope of Article 1 of the First Protocol stating that the notion "possessions" has an autonomous meaning which is certainly not limited to ownership of physical goods: certain other rights and interests constituting assets can also be regarded as «property rights», and thus as "possessions", for the purposes of this provision"<sup>71</sup>. Intellectual property has thus joined other intangible assets<sup>72</sup>, held by the ECHR to amount to *possessions* protected by the Convention's right to property.

The position is that, in case of trademarks<sup>73</sup>, and supposedly also patents, not only registered rights, but also mere applications for registration are protected by

69. *Dima v. Romania*, App. No.58472/00, para. 87 (admissibility decision).

70. *Anheuser-Busch Inc. v. Portugal*, App. No.73049/01, Eur.H.R.Rep. 42 [846], 855-856 (Chamber 2007) (judgment of 11 October 2005).

71. *Gasus Dosier-und Fordertechnik GmbH v. The Netherlands*, Application 15375/89 (1995).

72. Other intangible assets that amount to *possessions* according to the rulings of the European Court of Human Rights include e.g. various licenses, contractual rights, leases and business goodwill. See çoban A.R. (2004), *Protection of Property Rights within the European Convention on Human Rights*, Ashgate Publishing Ltd., Aldershot, p. 152-155.

73. See *Anheuser-Busch Inc. v. Portugal*, App. No.73049/01, Eur.H.R.Rep. 42 [846], 855-856 (Chamber 2007) (judgment of 11 October 2005).

the Convention's right to property. This is also consistent with the earlier well-established case law of the ECHR for the Court has extended the temporal scope of Article 1 to both current and future proprietary interests by stating that the "possessions" can be either "existing possessions" or assets, including claims, in respect of which the applicant (...) has at least a "legitimate expectation" of obtaining effective enjoyment of a property right"<sup>74</sup>.

What then is the nature of the human right to property to which the status of the protection of intellectual property has been elevated by the case law of the European Court of Human Rights and what are the implications of such an approach for the vision of knowledge creation and diffusion in European human rights law?

The previous section of this paper has already indicated that the human right to property as regulated in Article 1 of the Protocol 1 to the European Convention differs significantly from the right to property derivable from comparative research in private law. The very wording of the provision itself, using interchangeably the expressions: "possessions and property", suggests it varies considerably from the private law regulations on property. Firstly, it is the result of a discrepancy in this respect between the common-law and the continental legal traditions that are both represented by the parties to the European Convention.<sup>75</sup> Secondly, it is due to the specific function of the protection of property on the human rights level, which is a constitutional type of protection. Contrary to the norms on property in private law, it does not regulate legal relations between individuals with regard to commodities, but instead protects a private party's right to property against the state.<sup>76</sup> By the same token, the human rights' definition of property is considerably broader than its private law equivalent and covers all patrimonial rights that have economic value<sup>77</sup>. Moreover, it protects all pecuniary rights arising from private and public law relationships and legitimate expectations of those rights of both natural and legal persons.

Although primarily the right to property regulated in Article 1 of the Protocol 1 to the European Convention refers only to the vertical relationship between

---

74. *Kopecký v. Slovakia*, App. No. 44912/98 (2004) Eur. Ct. H.R., p. 139-140, Cited after L. R. Helfer (2008). FN 39, p. 33.

75. Popović D., (2009), *Protecting Property in European Human Rights Law*, Eleven International Publishing, p. 14.

76. Çoban A.R. (2004), p. 31.

77. The human right to property in the European Convention on Human Rights could be described as covering "universality representing the whole of the person's assets and liabilities assessable in monetary terms", Lametti D. (1998), *The Deon-Telos of Private Property: Ethical Aspects of the Theory of and Practice of Private Property*, unpublished D. Phil. Thesis, Oxford, p. 33; quoted after: Çoban A.R.(2004) p. 13.

private parties and the state, it does also concern the horizontal dimension in as much as the state is responsible for regulating private relationships.<sup>78</sup> Due to this influence on the relationships between private parties, the adjudication of the ECHR by recognising the *human-right-to-property* status of intellectual property and equating it with other protected *possessions*, treats the works of human ingeniousness as private or at least club goods.

The attitude of the European Court of Human Rights towards the protection of interests in intellectual creations must therefore be regarded as completely different from the regulations of the Universal Declaration of Human Rights and the International Covenant on Economic, Social and Cultural Rights analysed above. Unlike these two instruments of universal human rights law, the European Convention does not provide a mechanism that would expressly balance the rights of individual creators, on the one hand, and the right of the public, on the other. In its rulings, the European Court of Human Rights refers directly to various types of IP rights as regulated in intellectual property law. Unlike the mechanisms of the UDHR and the ICESCR, the case law of the European Court of Human Rights, not only refers directly to intellectual property rights, but it also equates them with the right to property of tangibles. By doing so, the Court raises the rank of intellectual property to the level of a human right to property. Accordingly, it has taken the opposite approach to knowledge when between knowledge and compared to the approach of the Universal Declaration and the Covenant. Whereas the two documents of the universal human rights law recognise global public good's qualities of knowledge, the case law of the European Court of Human Rights seems to approach knowledge as a private or at least club good.

#### ***4.2 Article 17 of the Charter of Fundamental Rights of the European Union***

A similar approach to that present in the case law of the European Court of Human Rights was adopted in Article 17 of the Charter of Fundamental Rights of the European Union<sup>79</sup> which reads as follows:

Right to property

---

78. Çoban A.R. (2004), p. 170, (noting that "[I]f because of a law in force, an individual's property rights are affected adversely in a relationship between private individuals, a state should be held responsible, because there is the state's authority in all laws including that regulating private relationships").

79. Charter of Fundamental Rights of the European Union, 18 December 2000, (2000/C 364/1), entered into force 1 December 2009, (hereinafter the Charter or CFREU).

1. Everyone has the right to own, use, dispose of and bequeath his or her lawfully acquired possessions. No one may be deprived of his or her possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss. The use of property may be regulated by law in so far as is necessary for the general interest.
2. Intellectual property shall be protected.

Here the equation of intellectual property rights with the right to property in tangibles is even more evident: the notion of intellectual property is expressly used in the provision unambiguously titled the right to property. As the regulation of the Charter is similar to the reasoning of the European Court of the Human Rights, and bearing in mind the fact the Charter has just entered into force and hence the lack of significant case law in this field, this provision will not be analysed separately. Nonetheless, the vision of knowledge present both in the European Convention on human rights and the Charter of Fundamental Rights of the European Union will be jointly discussed in the following paragraphs.

## **5. Knowledge as a public or private good? A new twist to an old tale**

The opposition between the two approaches, with the Universal Declaration and the International Covenant on one hand, and the case law of the European Court of Human Rights and the regulations of the Charter of Fundamental Rights of the European Union on the other, closely resembles the discourse that has long been present in the domain of intellectual property law. The common question the two approaches pose is whether the most just and efficient model of protecting knowledge creation and dissemination should treat the works of human ingenuity as private or public goods. As mentioned in the introduction, the disagreement on this issue may be traced as far back as to various philosophical theories explaining the role, function and nature of intellectual property law. All the arguments developed afterwards in this dispute within intellectual property doctrine are equally valid for the human rights approach towards the protection of interests in intellectual creations and hence should be explored here. Nonetheless, due to the nature and constraints of this text, only the most crucial observations will be mentioned.

Private goods as opposed to public goods are excludable and rivalrous. Access to a private good is allowed only on the payment of the price, which is set by the seller. Those not paying cannot enjoy the benefits of private goods. This system leads to some inefficiency by excluding those individuals who cannot afford the price and who would otherwise have benefited from the resource. This seems,

however, justified and even inevitable, in case of goods which by their nature are scarce and their consumption is characterised by rivalrousness. Nevertheless, the opponents of the commodification of knowledge claim that this feature is not borne by the knowledge goods, which they perceive as a perfect example of non-rivalrous goods. On the contrary, due to network externalities, ideas may become more valuable to the society as a whole if they are used to the largest possible extent<sup>80</sup>. Moreover, unlike tangible assets, the products of the mind that are protected by intellectual property rights are also non-excludable in nature, as the substance of sharing the ideas, particularly in the digital era, is such that no one can easily be excluded from enjoying the information. Furthermore, as the marginal cost of the knowledge goods reproduction in digital era is close to zero, they are also not scarce in their nature - it is intellectual property law that artificially creates this scarcity. Therefore, such profound protection of the results of human ingeniousness, going as far as to equate it with the protection of property in tangibles, may not only be dangerous for the rights of the general public but also completely inadequate with respect to the nature of the intellectual creations.

Arguably, the monopoly in intangibles, as opposed to tangibles, is artificially created by the legal system and does not stem from the immanent features of those goods. Since products of mind are neither scarce and rivalrous, nor excludable in themselves, it is intellectual property law that creates scarcity and excludability where neither existed before<sup>81</sup>. At the same time, it redefines the characteristics of knowledge from those of a global public good into a private/club good. Due to the differences between tangible and intangible assets, and subsequently to the dissimilar social functions of the protection of property and intellectual property, these two legal concepts vary in their scope and temporal duration. Unlike the right to property, lacking temporal limitation and granting complete control over the owned items to possess, use and alienate them, intellectual property rights are both limited in time and scope<sup>82</sup>.

The essential divergences between the nature of tangibles and intangibles also confirm the completely different *raison d'être* of the right to property on the one hand and intellectual property rights on the other. Whereas the objective of the

---

80. Cornides J., (2004), p. 136.

81. Marlin-Bennet R., (2004), p. 13.; See also: Lemley M. (2004), *Property, Intellectual Property and Free Riding*, Working Paper no.291, Stanford Law School, p. 31, (asserting that: "[i]ntellectual property, then, is not a response to allocative distortions resulting from scarcity, as real property law is. Rather it is a conscious decision to create scarcity in a type of good in which it is ordinarily absent in order to artificially boost the economic returns to innovation").

82. E.g. fair use provisions in common-law and exceptions and limitations to copyright in continental law, impossibility of alienating the moral rights in some legal orders etc.

right to property is to prevent the over-use and depletion of scarce resources as well as to internalise the negative externalities connected with the owned good<sup>83</sup>, the aim of intellectual property protection is the enhancement of creation and innovation<sup>84</sup> together with a just recognition of the effort put into the creation of a knowledge good. The externalities stemming from knowledge goods are mostly positive, hence need not be internalised in the same manner as the negative externalities of the tangibles are internalised through the mechanisms of the property right.<sup>85</sup>

Consequently, intellectual property rights should not be equated with the right to property only because of the coincidence in nomenclature. At this point it should also be noted that the term “intellectual property” is of quite recent origin, dating back to 19th century and is much younger than the legal concept itself<sup>86</sup>. As argued by Fritz Machlup and Edith Penrose, its coining was “a very deliberate choice on the part of the politicians working for the adoption of a patent law in the 19th century. This period was for liberty and equality and against privileges and monopolies of any sort. Patent law on inventions based upon a “monopoly privilege” would be rejected, but as a «natural property right», the patent law would be justified or accepted.”<sup>87</sup> Therefore, as Jakob Cornides appropriately notices, the sheer nomenclature cannot misleadingly allow the “name of something influence [the] idea of what it [really]is.”<sup>88</sup>

In the light of the above, it should be asserted that treating the protection of intellectual and artistic works on equal footing with the right to property in tangible goods creates the risk of overprotection to the detriment of the general public, especially when it is expressed in the strong and overarching paradigm of human rights. Particularly challenging for the welfare of the community as a whole is the attitude of the European Court for Human Rights due to the fact that “[w]ithin the European regional human-rights system, powerful companies no less than wealthy individuals may bring, and have indeed brought claims of violations of

---

83. See Lemley M. (2004).

84. Cornides J. (2004), p. 150.

85. Lemley M. (2004), p. 32, (asserting that: “the «problem» of intellectual property differs fundamentally from the problem of real property law. It is the problem of internalizing positive rather than negative externalities”).

86. See: e.g.: Vaidhyanathan S. (2001), *Copyrights and Copywrongs: The Rise of Intellectual Property and how it Threatens Creativity*, New York University Press, p. 21; Fisher W.W. III, (1999), *The Growth of Intellectual Property: A History of the Ownership of Ideas in the United States* in: “Eigentum im internationalen Vergleich” Vandenhoeck & Ruprecht, pp. 2, 8.

87. Machlup F. and Penrose E., (1950), *The Patent Controversy in the Nineteenth Century*, Journal of Economic History X (1), May 1-29; cited after Cornides J., (2004), FN 47, p. 146.

88. Cornides J. (2004), FN 47, p. 146.

their “human” rights before the European Court of Human Rights”<sup>89</sup>. In fact, unlike the UDHR, ICESCR and CFREU, the European Convention protects not only intellectual and artistic creations of individual authors and inventors, but covers also interests of legal persons, including potent multinational corporations.

Hence, the attitude of the European Court for Human Rights could be regarded as significantly different from those present in the Universal Declaration and the Covenant, and further, as less suitable for the maintenance of the fragile balance between the rights of creators and inventors on the one hand and the rights of the general public on the other.

However, it should be stressed that the right to property enshrined in Article 1 of the Protocol No. 1 to the European Convention is not absolute and unlimited. This conclusion could be drawn from the very wording of the provision, recognising the public/general interest as the limit of the right to property. This reasoning is confirmed also by the drafting history of this Article, well illustrated by the statement of the Belgian MP, De la Vallée-Poussin, who described the prevailing attitudes of the drafters towards the notion of property as follows: “No longer does any party defend the absolute right to own property, as it was understood by Roman law, and I do not think there is anyone either who is in favour of the completeness of the Communist theory.”<sup>90</sup> Further confirmation of this stance may be found in the well-established case law of the ECHR recognising “functional importance of particular rights in democratic societies, the rationales governments advance for restricting those rights, the arguments for and against deference to domestic decision makers, and the need for the Convention to evolve in response to legal, political and social trends in Europe”<sup>91</sup>.

The social conception of both the state and the function of property<sup>92</sup> present in the case law of the ECHR<sup>93</sup> therefore may well achieve the same goal as the

89. Scott C. (2001), *Multinational Enterprises and Emergent Jurisprudence on Violations of Economic, Social and Cultural Rights* in Eide A., Krause C. and Rosas A., (eds.) (2001), *Economic, Social and Cultural Rights: A Textbook* 2<sup>nd</sup> rev. ed. Martinus Nijhoff Publishers.

90. European Court of Human Rights, Preparatory Work on Article 1 of the First Protocol to the European Convention on Human Rights – Information Document prepared by the Registry, 1976, p. 6, quoted after: Popović D. (2009) p. 6.

91. Helfer L. R. (1998) *Adjudicating Copyright Claims Under the TRIPs Agreement: The Case for a European Human Rights Analogy*, Harv. Int'l L.J. 39, p. 407, emphasis added.

92. Scott C. (2001), p. 564.

93. For examples of the ECHR's decisions based on the concept of social justice and the social function of property See: Popović D., (2009) pp. 140-144, (where he lists inter alia: *James and others vs. United Kingdom*, Judgment of 21 February 1986, ECHR (1986) Series A, No. 98 (1986); *Lithgow and others vs. United Kingdom*, Judgment of 08 July 1986, ECHR (1986)

mechanism inbuilt in the UDHR and ICESCR. Analogous reasoning is equally valid for the Charter of Fundamental Rights of the European Union, as its Article 17 clearly limits the right to property by the general interest of the community. Consequently, both property right and intellectual property rights, though much different in substance, are not “an end in [themselves and] must be used in a way that contributes to the realisation of the higher objectives of human society.”<sup>94</sup>

Therefore, in conclusion, the human rights' analysis of the protection of knowledge creation and diffusion, no matter if approached from the knowledge -as-a-global-public-good knowledge-as-a-private property perspective, might be useful in setting the barriers to the graining body of intellectual property law that increasingly heats the protection of the right holders as absolute and infinite, whilst the rights of the public.

---

Series A, No.102; *Gaygusuz v. Austria*, Judgment of 16 September 1996, ECHR Reports 1996-IV; *Oneryildiz v. Turkey*, Judgment of 30 November 2004, ECHR Reports 2004-XII; *Hutten-Czapska vs. Poland*, Judgment of 19 June 2006, ECHR Reports 2006;etc.); See also generally Tulkens F., “*La réglementation de l’usage des biens dans l’intérêt général. La troisième norme de l’article 1er du premier Protocole de la Convention européenne des Droits de l’Homme*” in: H. Vandenberghe (Ed.) (2006) “*Property and Human Rights.*” Brugge die keure la charte-Bruylant; A. van Rijn, “*Right to the Peaceful Enjoyment of One’s Possessions*” in van Dijk P. et al. (Eds.) (2004), *Theory and Practice of the European Convention on Human Rights* 864.

94. Cornides J., (2004), p. 143.



# **Institutional open access repositories in college education: a proposal for their role in open educational resources in Greece**

---

---

**Nikos Koutras, Elisa Makridou & Iliana Araka**

---

---

“Every society has resources that are free and resources that are controlled.  
A free resource is one that anyone equally can take; a controlled resource  
one can take only with the permission of someone else.  $E=MC^2$   
is a free resource. You can take it and use it without the permission  
of Einstein estate. 112 Mercer Street, Princeton, is a controlled resource.  
To sleep at 112 Mercer Street requires the permission  
of the Institute for Advanced Study”

*Lessig, 2002*

## **1. Introduction**

There is an increasing interest for the creation of open access repositories both at the national and transnational level, through European programs and cooperation initiatives. Information should be provided in the best possible way to all end users, at the proper quality and size. As members of the Information Society, we realize that there is a constant effort to overcome certain obstacles – both at the transnational and national level – that impede information access.

One could initially address the issue of Open Educational Resources, through registering and shortly analysing open access repositories as a political phenomenon. This view is supported by the fact that politics can be viewed through three different angles, and more specifically as a relationship, a value or a process (Kouskouvelis, 1997). Thus, certain relationships are being established among end users, information scientists, trainers and trainees in educational institutions and a large number of other actors that wish to exchange information through digital repositories.

The value of this process stems from the basic model on which digital repositories are ‘built’: the open access model. As Zmas (2007) puts it: “...knowledge and information can now be found at the heart of the European university”. This process starts with the establishment of a methodology that is being followed up to the final integration of print information into the information ‘reservoirs’ of

digital repositories. Print documents include books, magazines, conference minutes, scientific papers etc.

It is thus quite obvious that the future of information lies mainly upon the correct use of technological developments. However, there seems to be a certain amount of reluctance on the part of universities, concerning the use of open access information and digital repositories. This phenomenon is mainly due to scientific community's lack of adequate information to evaluate the progress of their deposited documents.

Despite this reluctance there seems to be an increasing intention to create and properly manage open access repositories in Greece, attested by the increasing amount of recently founded Greek digital repositories. The key elements for the development of those repositories lie in providing adequate information to the administration and scientific staff of universities, so as to promote the complete integration of this new information model.

## **2. Designing the Education of the Future**

### **2.1. *eEurope***

The transition to a digital information economy is considered to be fundamental for financial development, competitiveness and employment in the EU. Furthermore, it is expected to improve the life quality of EU citizens and protect the environment.

In order to create a wide "Information Society" the Committee launched the eEurope initiative in December 1999, an ambitious project aiming at spreading Information and Communication Technologies (ICTs). The main objectives of this initiative were:

- Introducing European citizens into the digital era and online.
- Building a digitally literate Europe, supported by an entrepreneurial culture, and
- Making sure that the process is socially inclusive and builds consumer trust.

### **2.2. *1st phase: eEurope 2002***

The eEurope 2002 action plan was adopted by the Feira Council in June 2000 and is part of the Lisbon Strategy for financial, social and environmental reform. The plan was updated with eEurope+, which was launched following an appeal by the Feira Council for the adoption of the Lisbon strategy. The action plan included 11 fields of action and 64 goals that should be reached by the end of 2002 (European Commission, 2003).

The eEurope 2002 action plan was generally quite successful in bringing European citizens and businesses into the digital era and online, as well as in establishing a framework for the development of a knowledge economy. More specifically:

- A significant increase in internet connectivity was observed, and
- A legal framework was established for online communication and e-commerce.

If Europe wishes to create a knowledge economy, it should invest in the modernization of education and provide schools, teachers and students with an easy access to high quality information and communication resources.

The progress marked during the first phase of the eEurope initiative, through the eEurope 2002 action plan, in improving school internet services and providing computer equipment for staff members and students, has been quite significant. Annual surveys that were conducted in order to monitor educational improvements as perceived by the teaching and administrative staff, produced the following results (European Commission, 2003):

- Computer equipment levels within the EU are high and constantly increasing.
- The main factor influencing the levels of computer equipment is the level and type of education.
- 93% of the schools were already connected to the internet since February 2002.
- As regards bandwidth, narrowband connections seem to be more common. However, since late 2002, broadband connections have been constantly increasing.
- Since late 2002, more than half of the EU teachers have been formally trained in the use of computers and four out of ten know how to use the internet.

Schools are increasingly interested in electronic educational products and services and the framework of their use. Their interest exceeds connectivity and infrastructure issues and touches upon issues of content, teacher training, consequences on organizational structures, as well as new social impacts outside of the educational environment.

### **2.3. 2nd phase: eEurope 2005**

This action plan is the successor of eEurope 2002, following the same approach and setting specific goals. The eEurope 2002 action plan aimed at improving in-

ternet connectivity in Europe, which could be «interpreted» into an increase in relevant financial activities. This was the actual focus of the eEurope 2005 action plan. It aimed at accelerating the creation of new legislative frameworks and reorienting the already existing programs, based on certain priorities. More specifically, it aimed at: boosting services, applications and content that can create new markets and minimize costs. The plan focused on fields where politics could provide added value and contribute to the creation of a positive environment for private investments (European Commission, 2002).

The goals of eEurope 2005 can be summarised as follows (they were to be achieved by the end of 2005):

1. Modern public internet services
2. Electronic government services (eGovernment)
3. Electronic education services (eLearning),
4. Electronic health services (eHealth),
5. An active electronic environment for businesses (eBusiness)

And in order to achieve the above mentioned goals:

- Wide broadband connectivity in competitive prices
- Secure information infrastructures

The action plan was structured around four interconnected lines (European Commission, 2002):

1. Political measures in order to reform and adapt legislation, at the national and regional level, promote competitiveness and interoperability, raise awareness and express political will.
2. Measures that should be based on the development, analysis and diffusion of best practices.
3. Measures that focus on a comparative evaluation of the progress marked, and
4. The coordination of existing policies and proposed actions.

Ever since its first implementation, the eEurope initiative has had a wide political impact, reinforcing existing initiatives and promoting the creation of new ones. One of its main principles was the establishment of policies at the European, national and regional level.

E-initiatives and support programs are now very common within the EU, and are even being launched by individual member-states and regions. The example of

the EU has been followed by other geographically European and candidate countries, such as Norway with the eNorway initiative.

## ***2.4. The eLearning program (2004-2006)***

The eLearning program was mainly based on the eLearning action plan 2001-2004, approved on May 24 2000 (European Commission, 2001, 173), and the eLearning initiative (European Commission, 2000, IP/00/522). The initiative's main goal was to optimize the use of new technologies, multimedia and the internet, as well as to improve the quality of education and facilitate access to information services. The program aimed at supporting and further developing ICTs in education and training. Its main aim was to promote high quality education and address the needs of the knowledge society through a lifelong learning framework (European Commission, 2009, 159).

The available budget for the period 2004-2006 amounted to 44 million Euros, 45% of which was used to finance the collaboration of schools through ICTs (the eTwinning project). New organizational models were developed in order to create virtual educational spaces and add a virtual dimension to the European University Cooperation. Digital literacy was further reinforced through the promotion of all the necessary skills required in an information society.

The program was extremely successful in achieving short-term benefits for several institutions. Over 98% of the eLearning coordinators surveyed believed that their projects had a positive impact on improving cooperation among institutions. Other benefits of the program include transnational cooperation, communication and exchange of best practices. The eLearning program was also quite effective in producing positive results for staff-members and teachers. 75% of the respondents agree or totally agree that their projects had a positive impact on the quality of teaching, learning and the curriculum (European Commission, 2009, 159).

Overall, the eLearning program has positively contributed to the goals of Education and Training 2010. It produced significant results in promoting knowledge society skills and reinforcing access to ICTs. 67% to 75% of the respondents agree or totally agree that their projects contained significant models of digital literacy (European Commission, 2009, 159).

The eTwinning program has been extremely successful in creating an innovative and interesting free access model for schools, through the eTwinning portal and a peer browsing service, as well as through the organization of projects at the school level and the promotion of educational counselling and best practices. This approach has proven to be quite popular for the target public and extremely cost-effective. The program has actually exceeded expectations for participation and popularity.

The eLearning activities are now part of the EU lifelong learning program. The eTwinning is part of the Comenius program and virtual educational spaces are part of the Erasmus program.

### ***2.5. The i2010 Initiative***

The i2010 initiative is an effort of the Committee to respond uniformly to the needs of the information society and establish legal frameworks for the audio-visual sector in Europe. The initiative aims at coordinating the actions of member states, in order to achieve digital convergence and address challenges linked to the information society. In order to form this strategic framework, the Committee 'drew inspiration' through a large scale debate of all interested parties, concerning older initiatives such as eEurope, eLearning, eTwinning etc.

The Committee proposes three priority goals that should be achieved by the end of 2010 through European policies at the fields of information society and the media (European Commission, 2005, 229). More specifically, the initiative aims at: creating a unified European information space, reinforcing innovation and investments in ICT research and developing an information and media society, based on social integration.

The Committee wished to create a more open and competitive internal market for information society and the media. The first aim of the i2010 initiative was to create a unified information space, providing accessible and secure communication, differentiated and high quality content and other digital services. In particular, the Committee was aiming at achieving the following:

- Faster broadband services in Europe.
- Encouraging the introduction of new internet services and contents.
- Promoting equipment and platforms that "talk to one another", and
- Making the internet safer against fraudsters, harmful content and technology failures.

In order to create a unified European information space, according to the i2010 initiative, the Committee proposes to (European Commission, 2007, 694):

- Revise the regulatory framework on electronic communications, so as to include an effective strategic management of the radio spectrum.
- Create a cohesive framework for the services of information society and the media.
- Provide constant support to the creation and diffusion of European content, such as eLearning, eContentplus and all future initiatives.

- Define and implement a strategy that promotes a safe European information society, mainly through self protection, threat monitoring, rapid and effective response to attacks and system failures, and
- Organize and promote targeted action on interoperability issues and especially on digital rights management.

## **2.6. The OLCOS Project**

As part of the EU electronic education initiative (eLearning), open educational content monitoring services –i.e. the OLCOS Project – implement a series of actions that aim at reinforcing the creation, widespread use and reuse of Open Educational Resources (OER) in Europe and throughout the world. The OERs include teaching and learning content, tools based on specific software and services, as well as licences that allow the development and reuse of content, tools and services (Geser, 2007). This project wishes to present the existing situation and possible future developments on OERs, while recording a series of proposals and strategies to address the existing issues.

Despite the fact that the results expected from the OLCOS project may support government and institutional decisions, there is a strong need for a strategic leadership in decision-making processes, so as to implement measures that further promote educational practices and open educational resources. OERs are a key factor for decisions that aim at reinforcing education and lifelong learning within the information society and economy. However, the project insists that it is equally important to promote innovation and bring about change in educational practices (Geser, 2007).

The OLCOS project provides significant information on OERs. More specifically, it is quite clear that if OERs are implemented in the prevailing teacher-centered educational model, both students and teachers will be able to develop the necessary skills and knowledge, so as to actively and efficiently participate in the information society and economy.

It is clear that there is an urgent need to reinforce open access teaching and learning practices, on the basis of an educational framework that promotes the development of all the required skills. Nevertheless, it is obvious that progress in this field can only be achieved in the long run, gradually and at the right 'pace'. Change can be brought about only with targeted and sustainable efforts by politicians and other actors responsible for shaping educational policies.

## **2.7. Conclusions**

New information and communication technologies (ICTs) deeply affect the ways in which we obtain information, communicate and learn. The challenges for edu-

cation and training are multifaceted and touch upon different parts of society (European Commission, 2001). These technologies entail challenges for the industry, which uses and produces them; challenges for employment, since it creates new professions and professional skills; and finally, cultural challenges, with the development of new internet services that affect cultural habits and are considered to be either a threat or a chance to achieve cultural and social diversity.

Challenges for education are equally important. Nevertheless, innovative technologies should explore their full potential for the benefit of education and prove their effectiveness in different learning fields, respecting linguistic, cultural and social diversity.

Furthermore, financial challenges are definitely present in the field of education. The use of ICTs should adjust to different educational goals and existing financial means, in order to strike a balance between infrastructure, education, content and human resources.

The fact that education can be found at the heart of innovation and EU decisions, demonstrates the significance of this field for the implementation of ICTs. Actually, it seems that the concept of education has become a 'pillar' for information accessing.

### **3. Looking into today's education**

ICTs are changing education by helping broadening access to educational materials. Many new services and products have been developed for this purpose, such as Virtual Learning Environments (VLEs), digital repositories and Open Educational Resources (OERs), and many institutions have been changing the course of education towards a more open model for accessing educational information. Looking profoundly into today's education, there is a new trend, that is OERs.

According to Madden (2010), there is no need for an institution to create OERs if they can't be shared. But what is exactly an Open Educational Resource and how is related to Institutional Repositories and Open Access?

According to OLCOS Roadmap 2012 (Geser, 2007) there is no accredited definition of OERs, but the following core attributes would characterize any possible OER definition:

- access to open content (including metadata) is provided free of charge for educational institutions, content services, and the end-users such as teachers, students and lifelong learners;
- that the content is liberally licensed for re-use in educational activities, favorably free from restrictions to modify, combine and repurpose the con-



tent; consequently, that the content should ideally be designed for easy re-use in that open content standards and formats are being employed;

- that for educational systems/tools software is used for which the source code is available (i.e. Open Source software) and that there are open Application Programming Interfaces (open APIs) and authorizations to re-use Web-based services as well as resources (e.g. for educational content RSS feeds)

Atkins, Brown and Hammond (2007), in their report to The William and Flora Hewlett Foundation proposed the following definition: OER are teaching, learning, and research resources that reside in the public domain or have been released under an intellectual property licence that permits their free use or re-purposing by others. Open educational resources include full courses, course materials, modules, textbooks, streaming videos, tests, software, and any other tools, materials, or techniques used to support access to knowledge.

According to UNESCO (2002) the recommended definition of Open Educational Resources is: The open provision of educational resources, enabled by information and communication technologies, for consultation, use and adaptation by a community of users for non-commercial purposes.

Wikipedia (2011) defines OERs as *digitized materials offered freely and openly for educators, students and self-learners to use and reuse for teaching, learning and research*.

One could easily assume the relation of Open Access and Open Educational Resources. But, let us document the term of Open Access as National Documentation Center (2011) of Greece defines it: *Open Access is the open, direct, constant and free of charge and most of the legal intellectual property limitations internet access to digital academic and scientific content. Users can use freely the available material for educational and other purposes*.

Thinking of the above definition and having in mind what an OER is, it is understood that both terms use within their definitions the words free, open, use and access alone or combined as phrases, meaning that both the movement of OA and the OERs refer to the fact that one can access freely scientific and educational content, respectively. Furthermore, the principle underlying both terms is summed up to the following statement: the commitment to the value and quality of research and educational information carries with it a responsibility to extend the circulation of this work as far as possible, and ideally to all who are interested in it and all who might profit by it (Willinsky, 2005). However, in order for these materials to be accessed openly, it is presupposed that they are hosted in places that can support efficiently not only free access, but search and indexing functions, metadata administration and preservation and Intellectual Property Rights

management mechanisms; as well as established policies upon which all mentioned above can rely and function properly for the benefit of the end user.

Institutional Repositories (IRs) could play this role as they bring together all these supporting mechanisms. IRs fulfill four functions that are directly related to their content: They are institutionally defined; they contain a wide range of materials, scholar and educational, which represent the intellectual wealth of an institution; they are cumulative and perpetual, and thus act as an archive and open and interoperable (Crow, 2002 and Prosser, 2003). In Greece, Open Access IRs have developed mainly among colleges, as 21 Colleges run their own OAI IRs as shown on the following table (Georgiou and Papadatou, 2010):

No	Title	Organization	Content
1	<a href="#">Bibliotheca</a>	Technological Educational Institute of Crete	Grey Literature
2	<a href="#">E-Locus</a>	University of Crete	Grey Literature, Archives
3	<a href="#">EPRINTS server of the Computational Systems &amp; Software Engineering Laboratory</a>	University of Macedonia	Grey Literature
4	<a href="#">Anaktisi</a>	Technological Educational Institute of Western Macedonia	Grey Literature
5	<a href="#">Grey Literature of the Aegean University</a>	Aegean University	Grey Literature
6	<a href="#">AUTH Digital Collections</a>	Aristotle University of Thessaloniki	Grey Literature, Archives, Special Collections
7	<a href="#">Estia - Digital Repository of Harokopio University</a>	Harokopio University of Athens	Grey Literature
8	<a href="#">Eureka!</a>	Technological Educational Institute of Thessaloniki	Grey Literature, Archives, Journals Articles
9	<a href="#">Helios: Repository of the National Hellenic Research Foundation</a>	National Hellenic Research Foundation	Grey Literature, Archives, Journals Articles, Books
10	<a href="#">Psepheda</a>	University of Macedonia	Grey Literature, Archives, Journals Articles, Special Collections
11	<a href="#">DSpace at NTUA</a>	National Technical University of Athens	Grey Literature, Archives, Journals Articles, Special Collections
12	<a href="#">Dpt of Electrical &amp; Computer Engineering: Repository</a>	Aristotle University of Thessaloniki	Grey Literature
13	<a href="#">Digital Repository of Agricultural University of Athens</a>	Agricultural University of Athens	Grey Literature
14	<a href="#">Ktisis - Institutional Repository</a>	Technological University of Cyprus	Grey Literature
15	<a href="#">Nemertes - Institutional Repository</a>	University of Patras	Grey Literature
16	<a href="#">Pandemos</a>	Panteion University of Athens	Grey Literature, Archives, Journals Articles
17	<a href="#">Grey Literature of Democritus University of Thrace</a>	Democritus University of Thrace	Grey Literature
18	<a href="#">Grey Literature of Technical University of Crete</a>	Technical University of Crete	Grey Literature
19	<a href="#">Digital Library of the University of Piraeus</a>	University of Piraeus	Grey Literature, Archives, Journals Articles
20	<a href="#">Digital Library of the University of Ioannina</a>	University of Ioannina	Grey Literature, Archives, Journals Articles
21	<a href="#">Pergamos Digital Library</a>	University of Athens	Grey Literature, Archives, Special Collections

**Table 1:** OA IRs in Greece (Georgiou and Papadatou, 2010)

Does really Greece have OERs? Throughout this section a European case study will be presented to show the importance of hosting OERs in repositories and a descriptive study of the current state of educational resources in Greece will be

used to point out the need for further development regarding all matters concerning OERs.

### ***3.1. The case of OpenLearn***

A typical example where OER can be found is the educational repository of the UK Open University, called OpenLearn (OpenLearn, 2011). The Open University was the first distance education institution and the first UK university to join the OpenCourseWare Consortium (2011), that is a collaboration of higher education institutions and associated organizations from around the world that creates a broad and deep body of open educational content using a shared model (<http://www.ocwconsortium.org/>). This leadership but also the continuous development of its content, makes OpenLearn a worth mentioning repository.

OpenLearn is a website created from the UK Open University in October 2006. It is part of the Open Educational Resources (OER) project and its main concern is to provide free access to all Open University educational material throughout the world. It uses a Creative Commons Licence (Attribution-ShareAlike-NonCommercial). This means that anyone can share, amend and reuse the contributed material, but not for commercial use. In other words, the OpenLearn repository contributes in making new knowledge available to all, in allowing users to use and reuse (download, modify, translate, adapt) the educational material and in giving them the opportunity to collaborate so as to modify all this material.

In a Moodle-based virtual learning environment, the Openlearn hosts and gives free access to over 400 structured study units, divided into different disciplines such as Arts and Humanities, Business and Management, Computing and ICT, Education, Health and Social Care, Law, Psychology, Social Science, etc. All material is hosted in "LearningSpace". This area is enriched by learning and communicational tools that support the use of forums, instant messaging, video conferencing and blogging, tagging or labeling of content, learning journals, the creation of personal profiles, the creation of the visual representation of the resources, etc.

Moreover all users can contribute their own educational material using the LabSpace area of the site. OpenLearn declares that in LabSpace someone can:

- Access all the content and tools from the LearningSpace as well as archived materials that may be useful but need updating
- Download the learning materials in several formats and adapt them to suit his needs
- Upload her/ his versions to share with the LabSpace community.
- Set up a collaboration zone to work with others in creating materials (OpenLearn, 2011).

The first two years, OpenLearn managed to host over 8000 study hours of learning materials and this rising course still continues. In 2010 OpenLearn made another step forward, by giving access to a variety of topical and interactive content, even to educational videos and games. This was achieved when OpenLearn was merged with open2.net, the online learning portal from the BBC and the Open University (<http://www.open2.net/>) where the latter broadcasts. Moreover, all users can follow OpenLearn on Twitter (<http://twitter.com/openuniversity>) or find it on YouTube channels (<http://www.youtube.com/ou>), Facebook and iTunesU (<http://www.youtube.com/ou>). It is worth mentioning the feedback that users leave on some of the above social media, expressing the usefulness of OpenLearn: *I've found the resources here to be extremely useful. I'm currently in my first year of an undergraduate degree, but the materials available on Open Learn are a great supplement to that and are often more interesting than the stuff we cover in formal lectures/tutorials* (From repository's Facebook wall).

Web 2.0 technologies and other relative social applications along with OpenLearn's licensing model encourages replication of the content and enables interoperability with other provider's content management systems. Users have the ability to download and upload materials in various formats. This way, viral content is created and is accessible for remote communities around the world. The fact that viral content is created enhances the importance of OpenLearn repository adding value to its services (Wikipedia, 2011).

OpenLearn repository could form a paradigm for every institution that wishes to create OERs as it has developed all means and policies necessary for the supporting of OER sharing, the trait that distinguishes them from other similar resource types.

### **3.2. Monitoring ER in Greece**

#### **3.2.1. Methodology**

A descriptive study was conducted aiming at monitoring the current situation in Greece as far as the educational resources in college education are concerned. The study objective is to identify the amount and type of educational resources (open, locked, registration required courses), the types of software platform used and matters regarding metadata and IPR licences.

In order to reach the goals of this attempt, information was collected through an on-site (online) inspection of every college in Greece, on January 2011. The sampling covered the entire population of Greek colleges, according to official data provided by the competent ministry, and comprised a total of 38 colleges, 23 of which are Universities and 15 Technological Education Institutes (Ministry of Education Life long learning and religious affairs, 2011). The amount of the courses of each college was calculated separately resulting in a total of 18.527. This figure corresponds to visible

courses only, as some college VLEs don't give access to any data. Each course forms a unique entity, that is, every course is counted once even if it appears in more than one software platforms a college may use. The courses are divided into three categories, open, locked and courses that require registration. Open courses are those that give free access to every user, internal (student or college staff) and external (every internet user). Locked are the courses whose content is visible only to registered students under permission granted by their professor. Courses that require registration permit access to registered internal and/ or external users.

The collected data were processed using SPSS 17.0 and produced descriptive statistics. To analyze software type variable set with college type group variable, cross tabulation was implemented. Since the courses came from two different types of colleges possible differences among the three types of courses had to be examined. To evaluate the role of the college type, independent *t-test* was applied. It was found that college type plays no significant role to course type, as *p* resulted higher than 0,005. So, this information will not be further mentioned.

### 3.2.2. Results

Table 2 shows how many colleges have certain type of VLE software. Out of the 38 colleges that were studied in total, 15 correspond to technological institutions and 23 to universities. According to the results of Table 2, only 2 institutions have an IR where ERs can be found, while the VLEs are most popular. It appears that most colleges have at least one VLE and the most popular platform is the OpeneClass, as 24 out of 38 colleges use it. However, there are four colleges with no software platform at all.

		College Type		Total
		University	Technological Educational Institution	
Software type	Blackboard	2	1	3
	OpeneClass	13	11	24
	Dspace	2	0	2
	Moodle	4	3	7
	CoMPUs	1	0	1
	Claroline	0	2	2
	Custom	3	2	5
	N/A	4	0	4
	<b>Total</b>	<b>23</b>	<b>15</b>	<b>38</b>

Table 2: Software and College Type

Table 3 and Chart 1 show the software type frequencies. At this point, it should be made clear that there are institutions that use more than one platform. Also, there are some colleges that do not use a ready-made platform, but a custom one (13,2%). Among others, the 63,2% of colleges prefers OpeneClass and 18,4% Moodle.

		Responses		Percent of Cases
		N	Percent	
Software type	Blackboard	3	6,3%	7,9%
	OpeneClass	24	50,0%	63,2%
	Dspace	2	4,2%	5,3%
	Moodle	7	14,6%	18,4%
	CoMPUs	1	2,1%	2,6%
	Claroline	2	4,2%	5,3%
	Custom	5	10,4%	13,2%
	N/A	4	8,3%	10,5%
	<b>Total</b>	<b>48</b>	<b>100,0%</b>	<b>126,3%</b>

Table 3: Software Type Frequencies

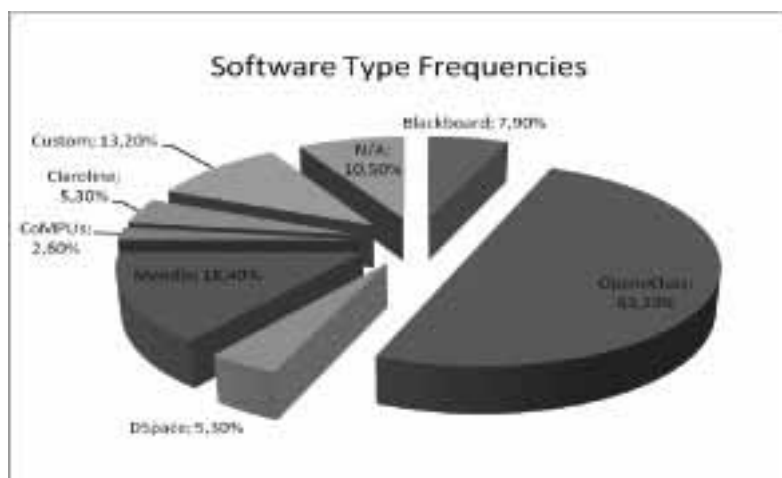


Chart 1: Software Type Frequencies

These platforms do not host only open educational material, but locked courses or courses that need registration too. In table 4 and chart 2 appear the total numbers and percentages of all courses that have been measured. It is found that

all courses are 18.527; Out of those the majority, 47%, are open, 19% locked and 34% courses that require registration. The mean of open courses in Greek colleges is 264,76 per college and the maximum value found in one entry is of 1351 open courses. It seems that open courses are more than half of the locked ones; however, comparing them to registration required courses they don't seem to have a significant difference that is a 13% more. The issue here is that it is not possible to know which of the registration required courses present the same characteristics to the locked ones – regarding level of access to students only (case of locked courses), nor the number of courses needing registration that allow any type of registered user to at least view the course material once registered to the course. In other case, there would be two categories of courses (open and locked) and the comparison would be clearer. Nevertheless, according to the figures of the chart 2, 47% still remains the highest percentage pertaining to open courses.

		Open courses	Locked courses	Registration required
N	Valid	33	33	33
	Missing	5	5	5
Mean		264,76	106,21	190,45
Std. Deviation		297,493	186,945	224,518
Minimum		0	0	0
Maximum		1351	779	967
Sum		8737	3505	6285

Table 4: Course type summary

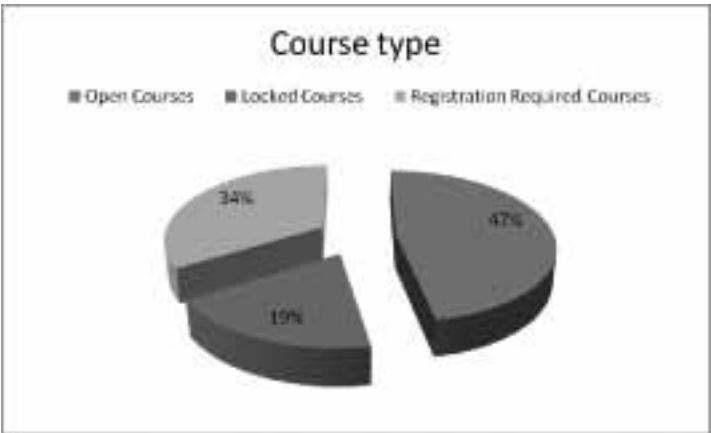


Chart 2: Course Type

As mentioned above (Table 2), there are only two universities that use among others DSpace to host ERs. DSpace software supports metadata schemas and Creative Commons Licences within the default deposit workflow. However, it was found that none of those two repositories assign Creative Commons Licences to their courses. Regarding metadata, both repositories support a Dublin Core schema; University of Patras repository supports LOM data model as well, though it seems that it has not been used so far. VLEs assign neither metadata nor CC Licences to their courses. Concerning content licences inspection showed that every college applies its own respective policy.

### 3.2.3. Conclusions

The findings of the study show that there is a great number of ERs, though according to the definition of an OER, these cannot be characterized as such. This happens because open courses are of free access but they cannot be shared. As a consequence, this educational trust, 47% of the total of courses studied, remains unexploited.

The ERs that have been studied here are hosted in a VLE, rather than a repository. It is understood that colleges trust mainly, among others, OpenClass software, which means that they prefer to use open software and that they seek after the respective support, since OpenClass has been developed by GUnet, the Greek Universities network. At the time being, those VLEs are not customized in a way that will allow sharing of content. Although the repositories studied use a software system that can support sharing, that doesn't apply, because the policies formulated prevent it from happening. Another finding is that repositories do not seem to be quite popular for the hosting of ERs, since the two colleges that have repositories use a VLE too; particularly, their VLEs host the majority of courses.

Sharing is not supported in any way, as each college applies its own policy. So, the concept of open content, in terms of access only, can stand, but the concept of OERs cannot. This is clear not only regarding educational material but the scholar one hosted in IRs as well. It is not the technological infrastructure that lacks, nor the know-how in building such services, but a central coordination concerning on how all this can be put together and function through a viable model that will allow a fair, as possible, adjustment to Information and Knowledge Society, that will consist of skilled citizens who will be equal to it.

It is obvious that a common central policy and a clear legal framework as far as OERs and repositories are concerned needs to be enacted, as a start point for every other change related to practical matters, such as semantic metadata creation, clear licensing statements and support, awareness raising campaigns, motivation issues regarding educational community, student engagement, etc., as explicitly listed in OLCOS Roadmap 2012 (Geser, 2007).



#### 4. Recommendations

As mentioned above, the number of ERs in Greece is remarkable, as it is also evident the interest for free access to the world's information and knowledge.

A crucial, therefore, proposal for the Greek educational repositories that host open access material could be any amendment and/ or addition of articles or paragraphs in laws 3191/2003 and 3369/2005. Law 3191/2003 refers to the national system that links vocational education and training to employment. Moreover, the law 3369/2005 complements the above mentioned one on the same topic.

Additions could be made to the Law 3369/ 2005 which concerns the systematic lifelong learning, a vital European vision for the Information Society and by extension for the Knowledge Society. So, in Article 2 of this Law, that lists the organizations that promote lifelong learning (colleges are included), it would be useful to get a new paragraph added legislating the Open Learning Repositories. This would give a separate substance to repositories recognizing them as providers of information services. This way, funding would be easier, as well as policy development. Furthermore, the way of functioning, the purpose and the assessment of OERs would be enacted by law. Therefore, the quality assurance of free information, provided through educational repositories in Greece, would be achieved immediately.

Alternatively, an article could be added to Chapter II of the same Law within the section *Other Provisions* that would refer to the Greek educational repositories exclusively. The above option offers the possibility of a mild adjustment to this law and thus to the attempt of quality assurance of information, as it was mentioned already. This way, a key institutional framework for the existence of the repositories and their nationwide operation under common rules could be achieved.

Provided the legal framework is regulated, a series of OER related tasks should be set out to form the landscape of educational change. Changes need to be human-centered and could, among others, include:

- Enhancement of OERs.
- Use of tools and services that promote collaborative learning.
- User – friendly design interfaces that allow easy access and resource search.
- Enforcement of open content initiatives.
- Engagement of teachers and learners in the development of learning tools.
- Clarification of Intellectual Property Rights and determination of the way a CC Licence is acquired, etc.

The prerequisite for these changes to be fruitful in Greek society is the promotion of educational practices that allow for acquiring competences and skills that are necessary to participate successfully in the knowledge society (Geser, 2007). This could be accomplished through the establishment of Information Literacy programs at all levels of education. Unfortunately, in Greece – at least in college education – such programs are very few as resulted by a research conducted in academic libraries. Respondents of the survey believe that more money is needed, the specialized library staff is not enough to run such programs and that there is a lack of appropriately equipped spaces (Korobili et al., 2008).

## 5. Further discussion

Currently, the Operational Program “Education and Life Long Learning” (Hellenic Republic et al., 2010) is taking place in Greece funding, through EE and the Greek state, the following actions:

- Amelioration of education at all levels of the Greek educational system
- Connection of education to the labor market
- Lifelong learning and
- Research

Through this program, within the Act “Digital action in higher education”, interested colleges are invited to lay down proposals about the creation of Open Educational Resources. At the same time, as a horizontal action, GUnet, the Greek Universities network will develop a central platform of hosting OERs, as well as the technical infrastructure and regulations that all participating colleges will have to follow. The Greek ministry of education has set as an example for the participants the initiative of MIT (Massachusetts Institute of Technology), “Open-Courseware” ([ocw.mit.edu/](http://ocw.mit.edu/)). The program will be completed in 36 months, namely by the end of 2014 a number of courses from the participant colleges will be of an OER format. So, for the years to come changes in education are expected and new data are to come up for research.

As of the results of this program it could be further discussed the idea of an on-line space where instructors all over Greece and/ or internationally could interchange opinions and share their educational material. A good example of how this could be done is the “Jorum repository” (Jorum, 2011). Jorum is part of and funded by JISC (<http://www.jisc.ac.uk/>). It is a service that collects and enables the sharing of learning and teaching materials, allowing their reuse and repurposing across the UK. This free online repository is intended to become part of the wider landscape of repositories. It stands as a national statement of the im-

portance of creating interoperable, sustainable materials, supporting individuals, teaching teams, collaborative groups and communities in the development and sharing of resources (JISC, 2009).

Jorum, a service in use – yet in development (JISC, 2011), could form a good example for Greece, as it was designed with a thorough human-centered logic. At the time the team behind Jorum reflected how the project would grow better concluded in a series of statements (Casey, 2008). It is worth mentioning the following:

- There is a need for clarity of purpose to support the sharing of learning and teaching resources.
- This clarity of purpose needs to be supported by an IPR and licence regime that enables the aims of the service and does not hinder it.

## References

- Atkins D., Brown J. and Hammond A. (2007), A review of the Open Educational Resources (OER) movement: achievements, challenges and new opportunities Online at [http://www.hewlett.org/uploads/files/Hewlett\\_OER\\_report.pdf](http://www.hewlett.org/uploads/files/Hewlett_OER_report.pdf)/accessed 21.01.2011
- Casey, J. (2008), Jorum Repository Case Study: Business Models and IPR Arrangements for Adopting an Open Access Service Online at <http://www.rsp.ac.uk/documents/case-studies/jorum.pdf> / accessed 01.02.2011
- Crow R. (2002), The Case for Institutional Repositories: A SPARC Position Paper Online at [http://scholarship.utm.edu/20/1/SPARC\\_102.pdf](http://scholarship.utm.edu/20/1/SPARC_102.pdf) / accessed 17.01.2011
- European Commission (1999), Communication: eEurope-An information society for all, Brussels, COM(1999) 687 final
- European Commission (2000), Communication: eLearning-Designing tomorrow's education, Brussels, COM(2000) 318 final
- European Commission (2000), Communication: The eLearning initiative, Brussels, IP/00/522
- European Commission (2001), Communication: The eLearning Action Plan-Designing tomorrow's education, Brussels, COM(2001) 172 final
- European Commission (2002), Communication: eEurope 2005-An information society for all, Brussels, COM(2002) 263 final

European Commission (2003), Communication: eEurope 2002-Final Report, Brussels, COM(2003) 66 final

European Commission (2005), Communication: i2010-A European Information Society for growth and employment, Brussels, COM(2005) 229 final

European Commission (2007), Communication: European i2010 initiative on e-Inclusion-To be part of the information society, Brussels, COM(2007) 694 final

Georgiou P. and Papadatou F. (2010), Scholarly Publishing & Open Access in Greece Online at <http://oaseminar.fecyt.es/Resources/Documentos/Greece2009.pdf> / accessed 24.01.2011

Geser G. (2007), Open Educational Practices and Resources-OLCOS Roadmap 2012 Online at [http://www.olcos.org/cms/upload/docs/olcos\\_roadmap.pdf](http://www.olcos.org/cms/upload/docs/olcos_roadmap.pdf) / accessed 05.02.2011

Hellenic Republic, and Ministry of Education, Lifelong learning and religious affairs, and European Union, and European Social Fund (2011), Invitation for proposal submission to the Operational Program “Education and Life Long Learning” Act “Digital Action in Higher Education”, Invitation code 101 Online at [http://www.edulll.gr/wp-content/uploads/2010/11/eclass\\_V73.pdf](http://www.edulll.gr/wp-content/uploads/2010/11/eclass_V73.pdf) / accessed 02.02.2011

JISC (2011), Jorum (at EDINA and Mimas) Online at <http://www.jisc.ac.uk/whatwedo/services/jorum.aspx> / accessed 18.01.2011

JISC (2009), JISC Services Case Study – Edina/Mimas Online at <http://www.jisc.ac.uk/whatwedo/services/about/casestudies/jorum.aspx> / accessed 18.01.2011

Jorum (2011), Jorum Learning to Share Online at <http://www.jorum.ac.uk/about-us> / accessed 19.01.2011

Korobili S., Malliari A. and Christodoulou G. (2008), Information literacy paradigm in academic libraries in Greece and Cyprus, *Reference Services Review*, 36 (2), 180 – 193.

Kouskouvelis I., 1997 “Introduction to Political Science and the Theory of Politics”, ed. PAPAIZI, Athens

Lessig L. (2002), The architecture of innovation, *Duke Law Journal*, 51, 1783.

Madden T. (2010), Turning a resource into an Open Educational Resource (OER) Online at [http://www.heacademy.ac.uk/assets/ps/documents/briefing\\_papers/oer.pdf](http://www.heacademy.ac.uk/assets/ps/documents/briefing_papers/oer.pdf) / accessed 22.01.2011

Ministry of Education Life long learning and religious affairs (2011) Online at [http://www.ypepth.gr/el\\_ec\\_category131.htm](http://www.ypepth.gr/el_ec_category131.htm) / accessed 10.01.2011

National Documentation Center of Greece (2011), Open access: knowledge for all Online at <http://www.openaccess.gr/openaccess/intro.dot> / accessed 05.02.2011

OpenCourseWare Consortium (2011), OCWare Consortium online at <http://www.ocwconsortium.org/> accessed 15.03.2011

Open University (2011), OpenLearn, online at <http://openlearn.open.ac.uk/> accessed 05.01.2011

Prosser D. (2003), Institutional repositories and Open Access: The future of scholarly communication, *Information Services & Use*, 23, 167–170.

UNESCO (2002), Forum on the Impact of Open Courseware for Higher Education in Developing Countries Final report Online at <http://unesdoc.unesco.org/images/0012/001285/128515e.pdf> / accessed 23.01.2011

Wikipedia (2011), Open educational resources Online at [http://en.wikipedia.org/wiki/Open\\_educational\\_resources#Other\\_Definitions](http://en.wikipedia.org/wiki/Open_educational_resources#Other_Definitions) / accessed 17.01.2011

Wikipedia (2011), OpenLearn, online at <http://en.wikipedia.org/wiki/Open-Learn> / accessed 17.02.2011

Willinsky J. (2005), *The access principle: the case for open access to research and scholarship*, The MIT press

Zmas A. (2007), *Globalization and Educational Policy*, Metaixmio

# **Building an inclusive information society at the local level in Estonia**

---

---

**Liia Laanes**

---

---

## **1. Introduction**

The development of information and communication technologies (ICT) has a significant impact on the public sector and citizen-state relations. It offers to the public sector additional possibilities to improve services and to involve citizens in decision-making.

Inclusion, in the context of information society and ICT can be understood at least in two ways. On the one hand, ICT can be an exclusion factor for certain groups in society and thereby inclusion or e-inclusion “aims at preventing the risk of digital exclusion, thus presupposing internet access and digital literacy” (Kettmann, 2008, p. 53). On the other hand, it also involves citizen participation, being more the issue of empowerment rather than access (eEurope Advisory Group, 2005, p. 5). In the Estonian public sector, e-inclusion is often defined as the use of the opportunities offered by information and communication technologies in order to make exercising public authority more transparent, comprehensible and inclusive for the society” (Reinsalu, 2010a, p. 8).

The aim of this paper is to analyse the information society and e-government in Estonia, particularly at the local level. This paper gives an overview of and examines the information society framework in connection with the Estonia's local governments. In addition, recent initiatives and developments in the field of information society at the local level will be examined in the light of these same developments at the state level. The main focus of the analysis is on the aspect of inclusion, since it concerns using ICT to improve the possibilities of residents to follow and be involved in the exercising of public authority.

## **2. Information Society and Democracy**

Information society affects public administration and democracy in several ways. The ICT has often seen to offer a possibility for improving internal managerial efficiency, the quality of service delivery (Moon, 2002) and responsiveness to citizens (West, 2004, p. 16), but also for increasing political participation (Macintosh & Whyte, 2008). Some have argued that we should not see it only as a possibility to improve the service delivery, but as “a new form of governance of

society, as it entails a new form of interaction among governments, citizens, the private sector, and community organizations" (Rodríguez Bolívar, Caba Pérez, & López Hernández, 2007, p. 144). "E-government can also be a tool to promote the positions of the government discouraging political debate and discussion" (Jaeger, 2005, p. 704).

One of the simplest definitions of "e-government" is that it refers to the production and "delivery of government information and services online through Internet or other digital means" (West, 2004, p. 16). The goal of the e-government "is to create a more dynamic government with far greater citizen involvement" (Streib & Navarro, 2006, p. 288). Broadly speaking, e-government includes four major aspects: "(1) the establishment of a secure government intranet and central database for more efficient and cooperative interaction among governmental agencies; (2) eeb-based service delivery; (3) the application of e-commerce for more efficient government transaction activities, such as procurement and contract; and (4) digital democracy for more transparent accountability of government" (Moon, 2002, p. 245). It is important to ensure that e-democracy is additional to, complementary to, and interlinked with traditional democratic processes and participative mechanisms, so as to widen the choices available to the public for taking part in political processes (Reinsalu, 2010b, p. 10; Höchtl, Parycek, & Sachs, 2011, p. 42). E-democracy can be divided into e-voting and e-participation; while the former can be viewed as a technological problem (Macintosh, 2004), the latter is usually associated with some form of decision-making (Sæbø, Rose, & Flak, 2008, p. 402). E-participation requires that services are provided by the government and citizens are using these services (Höchtl, Parycek, & Sachs, 2011, p. 32).

West (2004, p. 17) has proposed "four general stages of e-government development that distinguish where different government agencies are on the road to transformation: (1) the billboard stage, (2) the partial-service-delivery stage, (3) the portal stage, with fully executable and integrated service delivery, and (4) interactive democracy with public outreach and accountability enhancing features". Not all government websites go through these steps, plus they may undertake them in different order. Similar four or five stages models have also been proposed by several other authors (e.g. Layne & Lee, 2001; Charalabidis, Askounis, Gionis, Lampathaki, & Metaxiotis, 2006; Moon, 2002). In Moon's five stage model -based on degree of technical sophistication and interaction with users- the highest stage is political participation, which "requires highly sophisticated security, encryption, and interactive technologies to support online political participation such as election and public forum" (Moon, 2002, p. 428).

### 3. Strategy Documents and Legal Framework

In Estonia, e-democracy is a part of the Information Society Strategy. The first strategy document on information society was drafted as early as in 1994 and it was called "The Estonian Way to the Information Society". The next strategy documents were "Principles of Estonian Information Policy" (1998) and "Principles of Estonian Information Policy 2004-2006" (2004). The former document set out for the first time the principles for the development of the information society in Estonia (Ministry of Economic Affairs and Communications, 2006, p. 5).

A document adopted in 2006, "Estonian Information Society Strategy 2013", sets out 14 principles for the development of the information society. Among these principles is that "the development of the information society in Estonia is a strategic choice with public sector leading the way in pursuing its principles" (Ministry of Economic Affairs and Communications, 2006, p. 5). Until 2006, policies on information society have mainly focused "on the development of ICT infrastructure and the creation of systems necessary for implementing sectoral policies" (Ministry of Economic Affairs and Communications, 2006, p. 6). The "Estonian Information Society Strategy 2013" recognised the need to pay more attention to the citizen-centred and inclusive society. It stated that ICT is "an efficient tool for increased inclusion of citizens in public debates and decision-making processes" (p. 11), but it was also recognised that "participation in the information society requires, on one hand, multi-channel access to digital information and, on the other hand, skills and willingness to use the opportunities created as well as motivation to actively participate in decision-making processes" (p. 14). The implementation of the Strategy is based on annual Information Society Implementation Plans.

The Strategy for 2013 also contains some direct references to the local government. For example, it was expected that (Ministry of Economic Affairs and Communications, 2006, pp. 15, 19):

- Local governments will bring their websites into compliance with WAI quality criteria so as to ensure their accessibility for all, including people with special needs.
- Ministries and local governments will develop Internet-based environments for the inclusion of citizens and stakeholders in decision-making processes, in order to widen opportunities for participation in decision-making processes (e-democracy). Including the continual use of e-voting.
- There will be developed the necessary systems for increasing the efficiency of state and local government agencies, to improve the provision of e-serv-



ices at local level and avoid multiple development of similar solutions by different local governments.

It was not until 2008 that the Local Government Information Society Strategy was approved and special attention was paid to the coordinated development of information society and e-democracy at the local government level. The objectives for the development of information society at the local government level were drafted by the e-Governance Academy, which is a non-governmental organisation and founded for the creation of and distribution of knowledge concerning e-governance, e-democracy and the development of civil society. The preparation of the Strategy also involved different ministries and local government associations. In 2008 about 10% of local governments had their own ICT or information society strategy (Estonian Ministry of the Interior, 2008, p. 10).

The Local Government Information Society Strategy assumed that the introduction of e-services will make public services offered by local governments available to all, which would make governance to be more efficient and decisions to be more transparent (Estonian Ministry of the Interior, 2008). In the Strategy were formulated five objectives:

- All local governments implement digital procedure - they have electronic records management system, digital signature, digital procedures, and that information between authorities will be shared via electronic document exchange centre.
- All local governments have Internet-based possibilities to engage residents in the management of the local life - e.g. they have access via website to the decision-making process, which includes having an overview of what is happening at the council's session, being able to submit comments to the draft texts, and if need be, submit their own proposals for amendments to the drafts. All these operations would be done by using the ID-card.
- All civil servants of local municipalities will be aware of the possibilities to apply ICT tools in the information society.
- All local municipalities have established possibilities to use e-services.
- An organisation will be established to coordinate the development of the information society at the county level.

The legislation regulating the information society at the local level includes, for example, the following:

- Local Government Organisation Act (*Kohaliku omavalitsuse korralduse seadus*) - stipulates principles of local government among which are the right of the residents to participate in the exercise of local government and the transpar-

ency of local government activities (Section 3). Council regulations and resolutions and minutes of council sessions (Section 23(5)), minutes of rural municipality and city government sessions and of meetings of council and government committees under to the procedure provided for in the statutes of the rural municipality or city (Section 51(7)) have to be accessible to everyone. The Act was amended in 2010 and a provision was added according to which the development plan, together with the budget strategy and minutes of the council and council's committees meetings on the proceeding of the development plan, shall be published at the website of the municipality. The provision concerning the development plan is, at the moment, in this Act the only provision which contains a direct reference to the website.

- Public Information Act (*Avaliku teabe seadus*) - required local governments to have a proper website as of March 2002, and it also sets forth several responsibilities to the local governments in terms of disclosure and databases. For example, it requires a local government to disclose at its website economic statistics and forecasts, statutes of local government agencies and their structural units, formats of petitions and other documents submitted to local government agencies (and instructions for the completion thereof), research or analyses ordered by the local government agencies, etc.
- Digital Signatures Act (*Digitaalallkirja seadus*) - according to Section 4 of this Act, local government agencies "are required to provide access through the public data communication network to information concerning the possibilities and procedure for using digital signatures and digital seals in communication with such agencies and persons".

#### 4. Estonia - a leading e-state?

According to the recent statistical data of Eurostat (2011), 57% of Estonian population aged between 16-74 used the Internet frequently in 2010, which is slightly higher than the European Union average (53%), but remarkably lower than in the Nordic countries (e.g. 72% in Finland and 76% in Sweden). It has been argued that Estonia has gained the image of an advanced e-state because of the results of formal quantitative measures (e.g. number of Internet users, number of computers, and number of Internet connections), but the activities which individuals perform within online environments have been secondary (Runnel, Pruulmann-Vengerfeldt, & Reinsalu, 2009).

"Estonia has the largest functioning public-key infrastructure in Europe, based on the use of electronic certificates maintained on the national identification (ID) card" (The Freedom House, 2011, p. 129). The ID-card can be used for authentication, issuing digital signatures, electronic voting as well as many other func-

tions. The e-services provided at the state level have been gathered to a portal eesti.ee, which functions as a point of single contact. In 2010, about 63% of Internet users had used at least one e-government service (Randver, 2010). One of the most successful e-services at the state level is the e-tax office. In 2011, 95.3% of people who had to file their income tax return did it electronically (Estonian Tax and Customs Board, 2011).

In the democratic process, the best-known application is e-voting. Estonia was the first country in world to actually pass overall e-voting laws (Drechsler, 2004, p. 11). E-voting was first used for the local government elections in 2005 and for national elections in 2007. The number of people using this possibility is increasing with every elections. In 2005, at the local elections, 9,317 people decided to cast their vote by e-voting, yet at the parliamentary elections in 2011 the number was 140,486. This is 15.4% of the all eligible voters or 24.3% of the voters who decided to cast their vote (Estonian National Electoral Committee, 2011).

Although there have been at the national and international level several concerns about some aspects of e-voting, the raised concerns have not been considered, at least not publicly, to be serious enough to question e-voting in Estonia. The main concern is that the level of security is lower, compared to the regular voting, due to the possible insider attacks and computer viruses (Simons, 2010). Furthermore, voters have no possibility to verify whether their votes have been counted (Schryen & Rich, 2009) and there is a risk of intimidation and vote selling. There also are judicial barriers for redress. For example, in 2011, four e-voting related complaints were filed with the Supreme Court, but all these were dismissed on procedural grounds (e.g. the person's rights were not violated or the complaint was not filed within three days as of the resolution or act of the National Electoral Committee was performed)<sup>1</sup>.

E-Governance Academy described the situation of e-democracy in Estonia in 2010 by stating that the situation is excellent, but not hopeless (2010). Based on statistics, Estonia is doing well in terms of e-involvement and is far ahead of other countries with e-voting, but according to a survey in 2010 only 8% of the respondents had heard about the e-participation site [www.osale.ee](http://www.osale.ee) (E-Governance Academy, 2010), which was launched in 2007. Osale.ee is a successor to the portal TOM (*Täna Otsustan Mina* – Today I Decide). TOM was a public participation portal used in 2001-2008 and “aimed at engaging citizens more directly with the legislative and policy-making processes, either by proposing new legislation

---

1. See for example the judgment of the Constitutional Review Chamber of the Supreme Court of Estonia of 21 March 2011 in case 3-4-1-4-11 <<http://www.riigikohus.ee/?id=11&tekst=RK/3-4-1-4-11>> and of 23 March 2011 in case 3-4-1-6-11 (<http://www.riigikohus.ee/?id=11&tekst=RK/3-4-1-6-11>>).

or by suggesting amendments to existing laws” (Reinsalu, 2010b, p. 37). It has been considered to mark the beginning of e-democracy in Estonia (E-Governance Academy, 2007) and it allowed “citizens to discuss legislative proposals within a ten-day period following submission and to vote upon them” (Reinsalu, 2010b, p. 37). “The participatory website Osale.ee aggregates the legislative domains of all ministries and represents an attempt to consolidate different opinion seeking environments together under one roof” (Reinsalu, 2010b, p. 38). The portal TOM has been incorporated into Osale.ee. Allowing citizens to present ideas and proposals to the government, to ask other people to support the ideas (by collecting supporting “signatures”), to give opinion on the draft legislation that is being prepared and to perform searches among legislation and strategy documents.

The e-participation site osale.ee has 3,764 users as of April 2011; the number of active users is probably smaller, based on previous experience with TOM. TOM usage statistics between 2001–2006 shows that within 6 years it had about 6,000 users and about 1,000 legislative ideas were proposed, but only 45% of the users had performed any action (e.g. voting, proposing an idea, submitting a comment) after signup (Tallo, et al., 2007). The same study indicated that the 10 most active users generated 25% of all ideas. Tallo *et al.* highlight that e-participation in the case of TOM was hampered by lack of publicity, but also by the small number of positive responses.

There are also many different e-solutions in the public sector that have failed or were never implemented. Several IT-related projects have failed because of insufficient preparation. Weaknesses in the development of the State’s information systems have also been due to the minimal participation of the users in the development process and a lack of cooperation between ministries and agencies (National Audit Office of Estonia, 2010).

Kristina Reinsalu (2009, pp. 40-43) has divided the development of e-democracy in Estonia into three phases. The first was representative or institutional democracy, when the technological basis was created for the next phases. The second phase was consumer Internet democracy, which can be described as a focus on the development of e-services. The third phase, which has not occurred in Estonia yet, is participatory Internet democracy. Reinsalu explains this delay with the fact that though citizens are in the consumer phase and start to move to the next phase, officials and politicians are still in the first phase. The public sector has developed the services, but it does not motivate citizens to use these and does not provide help and guidance.

Government’s action programme for 2011-2015 includes an objective on information society to move focus from technology to the people. Related indicators increased the percentage of Internet users among the population aged 16-74 and

increased satisfaction of citizens and companies with State provided e-services. Planned, to this end, is to further develop e-services -both their quality and accessibility, e.g. by developing applications for smartphones-, but also to increase the coordination of the field by appointing a person who will coordinate the State's IT-policy. One of the most ambitious Internet-related sub-objectives is to become a global example for Internet-related legislation.

## **5. Local e-Government - From Websites to e-decision-making**

Estonia has a one-tier local government system. There are 226 local government units, of which 33 are cities and 193 rural municipalities. As of January 2011 the biggest is Tallinn with 411,903 inhabitants and the smallest is Pärnu with 101 inhabitants. About two thirds of the municipalities have less than 3,000 inhabitants. Despite the smallness of the country, the development of e-services at the local government level was predominantly uncoordinated until 2008. The National Audit Office concluded in 2006 that "the local authorities [had] not received sufficient support from the state in developing the information society" (2006, p. 1). A similar conclusion was reached also in 2007, when the National Audit Office (2007, p. 3) stated that if the State delegates responsibilities to the local governments, it should also provide the local governments with the relevant information systems to ensure even quality of the services.

### **5.1 Websites**

The simplest tool that local governments can use (and are obliged to use) to provide information and services over the Internet is a website. According to the Section 31(2) of the Public Information Act, the city and rural municipality governments were allowed to organise the maintenance of a joint website on the basis of a contract. The National Audit Office performed an audit in 2006 on the support the State provided to local authorities in developing the information society. One of the conclusions was that "the local authorities find it difficult to fulfil the requirements provided for in acts regulating administration of websites and disclosure of information on websites" (National Audit Office of Estonia, 2006). In March 2008, all the 227 local municipalities had a functioning website, but there were some deficiencies regarding updating of the information, website's poor structure, a lack of a search function covering its entire content, and difficult navigation (Estonian Ministry of the Interior, 2008, p. 9). Some examples of these problems can also be found today.

E-Governance Academy, involved in preparation of the audit report of the National Audit Office in 2006, studied local government websites also in 2009. Comparing the findings of the two studies, there had been considerable

progress in the introduction of comprehensive site maps and search engines, but at the same time the number of certain interactive web tools had decreased. For instance, the number of guestbooks (from 18% to 9%) and forums (in 2009, only 12% of the rural municipalities and 21% of the cities had a forum on their websites; the percentages used to be 25% and 33% respectively) had decreased (E-Governance Academy, 2009). A reason behind this trend was to forum comments that were often personally offensive and the quality of discussions were poor, though there were also forums with “fruitful debates” (Reinsalu, 2010a, pp. 8-9). While some municipalities have closed the forums, others (for example, Tartu) simply removed the possibility to comment on others’ questions, because there was too much slandering (Reinsalu, 2006).

An audit conducted by the National Audit Office on access to the information in local governments found “that the composition of data in document registers does often not comply with the requirements set by law and that finding the required document from the document register [on the website] may prove to be very time-consuming” (National Audit Office of Estonia, 2009). It is worth mentioning that the sample audited consisted of 15 municipalities and four different document register software were identified among the municipalities.

## ***5.2 Coordinated Projects***

Following the Local Government Information Society Strategy of 2008, the Estonian Ministry of Interior initiated projects for service portal for local authorities, as well as data security, records management, procedural environment for electronic documents, local councils’ e-decision making process, and spatial planning. Of these projects only the service portal and council’s information system have reached the testing phase. For example, the project on records management, which aimed to transition from paper to paperless management through the new system of records management faced several problems in 2009 (mainly related to the public procurement procedure) and has been postponed (Estonian Ministry of the Interior, 2011).

The service portal project (KOVTP) includes standardised structure for local government websites. It should facilitate the website management for the municipalities, but still leave them some possibilities to tailor their website according to their needs. Also it should transform traditional website into a service portal. The pilot project is complete and the service was made available to other municipalities in March, 2011. By the end of March around 40 municipalities had demonstrated interest to put the solution into use. The service portal should improve e-inclusion, because several functionalities have been added compared to current websites including services that require authentication with the ID-card.

The Government of the Republic has used the Information System of Government Sessions (called e-Cabinet) since 2000. It helps to save paper and time, because the length of the sessions has decreased from 4-5 hours to 30-90 minutes. In addition, all the documents and positions are available to all participants in real time (Government Office, n.d.). A similar solution has also been recently developed for local municipalities. A project called VOLIS was launched in 2009, which is an information system for local councils and governments. The project directly contributes to the second objective of the Local Government Information Society Strategy. The initial idea of the information system was generated among four counties, when they defined which information systems should be developed for local governments. The aim was to develop an application for local councils and governments, to integrate e-governance, participatory democracy, and records management (Pook, 2010). VOLIS covers all the procedures of the council. For example, it offers a possibility for council members to attend the council session virtually and, also, to vote. It also offers opportunities for citizens to follow the council session from their computers at home, read the documents of the session and launch initiatives. The latter is about proposing issues to the council to discuss or adopt and collecting supporting signatures for this proposal in VOLIS. As based on Section 32 of the Local Government Organisation Act "Not less than one per cent of the residents of a rural municipality or city with the right to vote ... have the right to initiate the passage, amendment or repeal of legislation of the rural municipality or city council or government concerning local issues; such initiatives shall be debated not later than within three months", it would facilitate acquiring the support of the one percent of the residents with the right to vote, as the link to the initiative can be shared via e-mail or social networking sites. In a later phase there will also be activated a possibility to give feedback to the draft (legislation) and to add comments, which both require identification with the ID-card (H. Pook, personal communication, April 11, 2011). Identification with the ID-card should avoid or at least reduce the problem of offensive comments and irrelevant comments, which is an inherent problem of forums. According to Pook (2011), the distinctiveness of the solution lies in the possibility for the council members to vote over the Internet using the functionality of the ID-card.

The software is not promoted among citizens and is not made available to them until it is sure that the local governments are ready to involve people. It is one of the precautions taken to mitigate the risk of failure of the project. Additionally, not all municipalities will start using the software at the same time, but when they are ready and willing to do it. Municipalities can choose whether they use the full possibilities or only some of the software's functions. For example, they

can use it only at the city government or council level and even then selectively (H. Pook, personal communication, April 11, 2011).

There are bottlenecks for the effective implementation of the system. An apparent one, is that some local municipalities do not have people who would be capable to make sure that all the required documents would be available via VOLIS and in time. Moreover, not all council members are computer literate and financial resources of municipalities are limited.

VOLIS and the service portal (KOVTP) are interrelated and municipalities themselves can decide whether and when they will start using the solutions. Taking up these solutions requires that local governments have the people who are capable to handle the systems, but it also requires (additional) financial resources as the VOLIS and KOVTP both are based on a monthly fee and there are additional costs that incur at the very first stage (e.g. training). Some municipalities have already considered the VOLIS and KOVTP to be too expensive for them due to lack of financial resources. The following year should show whether these two projects will be the next success stories or the lessons to learn from in e-government.

## 6. Conclusion

Estonia has several success stories to share with other countries in terms of e-government, but in practice the quality and user-friendliness of e-services is very heterogeneous and the level of e-government development at State level is clearly higher than local level. With the Public Information Act, the first stage of the e-government became mandatory for local governments in the year 2002. Even some years later, several of them presented problems to provide the required information on their websites.

Now, in a coordinated way, the State tries to help local governments to move towards a more inclusive information society and to offer citizens more tools for e-participation. Some municipalities in Estonia already offer possibilities to follow the council session online or to watch the recordings of the council session later, but it is more an exception than a rule. Coordinated development of the e-services not only enables developing more sophisticated solutions with fewer resources, but contributes also to technical interoperability of different solutions. It could be assumed that people should be more interested in participating in the decision making process on the local level issues than state level, but the question still remains whether the proposed solutions (e.g. VOLIS) will be attractive enough for citizens so as to be motivated to use the possibilities offered, whether their input would be constructive, and whether municipalities are able to create and sustain the dialogue.



There is still a lot to do to improve the security of the e-services, but also to raise citizens' awareness on the possibilities and tools they can use to participate in the decision making process at the local government level. The e-services enabling them to participate in the decision-making process (or in e-participation in general) have not been very successful in Estonia. A case study of Tartu, the second biggest city in Estonia, demonstrated that motivating people to use e-democracy services is much harder than ensuring access and services (Reinsalu, 2008). One main motivator behind the success of the e-tax office is a possibility to save time. In contrast, for e-participation there is no legal requirement to participate, participation assumes investing time and any positive results are not always visible, thereby it requires more efforts from the public sector to increase the motivation of the citizens.

## References

- Charalabidis, Y., Askounis, D., Gionis, G., Lampathaki, F. & Metaxiotis, K. (2006). Organising municipal e-government systems: a multi-facet taxonomy of e-services for citizens and businesses. In M. Wimmer, H. Scholl, Å. Grönlund, & K. Andersen (Eds.), *Electronic Government: LNCS* (Vol. 4084, pp. 195-206). Heidelberg: Springer.
- Drechsler, W. (2004). The Estonian e-voting laws discourse: paradigmatic benchmarking for central and eastern Europe. *ISPAcee Occasional Papers in Public Administration and Public Policy*, 5 (2), 11-17.
- eEurope Advisory Group. (2005). *e-Inclusion: new challenges and policy recommendations*.
- E-Governance Academy. (2007). *e-Demokraatia*. Retrieved April 5, 2011, from <<http://www.ega.ee/et/ega/e-demokraatia>>.
- E-Governance Academy. (2010). *Essee: Eesti e-demokraatia olukord aastal 2010 ning visioon aastaks 2015*. Retrieved April 5, 2011, from <<http://www.ega.ee/files/eDem%20essee.pdf>>.
- E-Governance Academy. (2009). *Kohalike omavalitsuste veebilehed e-kaasamise vahendina*. Retrieved March 16, 2011, from <[http://www.ega.ee/files/KOV\\_veebilehtede\\_analüüsi\\_kokkuvõte.pdf](http://www.ega.ee/files/KOV_veebilehtede_analüüsi_kokkuvõte.pdf)>.
- Estonian Ministry of the Interior. (2008). *Kohaliku omavalitsuse infoühiskonna arengukava aastateks 2008-2011 (KOV IYK 2011)*.
- Estonian National Electoral Committee. (2011, March). *Statistics about Internet Voting in Estonia*. Retrieved April 20, 2011, from <<http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics>>.

Estonian Tax and Customs Board (2011, April 8). *MTA tagastab tänavu maksumaksjatele 15,8 miljonit eurot vähem kui mullu*. Retrieved April 8, 2011 from <<http://www.emta.ee/index.php?id=29925>>.

Eurostat. (2011). *Individuals frequently using the Internet*. Retrieved March 27, 2011, from: <<http://epp.eurostat.ec.europa.eu/tgm/refreshTableAction.do;jsessionid=9ea7971b30dcd444cb6c0e42452ea1e2961f30d0b3e6.e34RaNaLaNOMc40LcheTaxiLbN8Se0?tab=table&plugin=1&pcode=tin00092&language=en>>.

Government Office. (n.d.). *Estonian e-cabinet*. Retrieved March 17, 2011, from <[http://www.riigikantselei.ee/e\\_cabinet/](http://www.riigikantselei.ee/e_cabinet/)>.

Höchtel, J., Parycek, P. & Sachs, M. (2011). E-participation readiness of Austrian municipalities. *Transforming Government: People, Process and Policy*, 5 (1), 32-44.

Jaeger, P. T. (2005). Deliberative democracy and the conceptual foundations of electronic government. *Government Information Quarterly*, 702-719.

Kettemann, M. C. (2008). E-inclusion as a means to bridge the digital divides: conceptual issues and international approaches. In W. Benedek, V. Bauer, & M. C. Kettemann (Eds.), *Internet Governance and the Information Society: Global Perspectives and European Dimensions* (pp. 51-61). Utrecht: Eleven International Publishing.

Layne, K. & Lee, J. (2001). Developing fully functional e-government: A four stage model. *Government Information Quarterly* (18), 122-136.

Macintosh, A. (2004). Characterizing e-participation in policy-making. *Proceedings of the 37th Hawaii International Conference on System Sciences*.

Macintosh, A. & Whyte, A. (2008). Towards an evaluation framework for eParticipation. *Transforming Government: People, Process and Policy*, 2 (1), 16-30.

Ministry of Economic Affairs and Communications. (2006). *Estonian Information Society Strategy 2013*.

Moon, M. J. (2002). The evolution of e-government among municipalities: rhetoric or reality? *Public Administration Review*, 62 (4), 424-433.

National Audit Office of Estonia. (2009). *Allowing and restricting access to information in rural municipalities and towns (Summary of an audit report)*. Retrieved March 27, 2011, from <<http://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?FileId=11030&AuditId=2087>>.

National Audit Office of Estonia. (2007). *Avalike teenuste kvaliteet infoühiskonnas*. Tallinn.

National Audit Office of Estonia. (2010). *Riigi infosüsteemide arendusprotsessi tulemuslikkus*. Tallinn.

National Audit Office of Estonia. (2006). *State support to local authorities in developing the information society (Summary)*. Retrieved March 16, 2011, from <<http://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?FileId=10932&AuditId=1955>>.

Pook, H. (2010). *KOV volikogu/valitsuse infosüsteem - VOLIS*. Seminar presentation at the Local Government Seminar on Information Society, 25-26 November 2010, Viljandimaa.

Randver, K. (2010, January). *Kodanike rahulolu riigi poolt pakutavate avalike e-teenustega*. Retrieved from <[http://www.riso.ee/et/files/kodanike\\_rahulolu\\_avalike\\_eteenustega\\_2010.pdf](http://www.riso.ee/et/files/kodanike_rahulolu_avalike_eteenustega_2010.pdf)>.

Reinsalu, K. (2010a). eInclusion in the local governments of Estonia. In Department of State Information Systems, *Information Society Yearbook 2009* (pp. 8-10). Tallinn: Ministry of Economic Affairs and Communications of Estonia.

Reinsalu, K. (2010b). *Handbook on e-democracy*. Tampere: Tampereen Yliopistopaino Oy Juvenes Print.

Reinsalu, K. (2006). Is Estonian local e-government responsive to citizens' needs? The case study of Tartu. *Information Polity* (11), 255-272.

Reinsalu, K. (2009). *The Implementation of Internet Democracy in Estonian Local Governments*. Tartu: Tartu University Press.

Reinsalu, K. (2008). *What are the factors of e-activeness in citizens' interaction with local government? A case study on online interaction in Tartu, Estonia*. Retrieved March 20, 2011, from <<http://www.iis.org/CDs2008/CD2008SCI/PISTA2008/PapersPdf/P511KZ.pdf>>.

Rodríguez Bolívar, M. P., Caba Pérez, C., & López Hernández, A. M. (2007). E-government and public financial reporting: the case of Spanish regional governments. *The American Review of Public Administration*, 37 (2), 142-177.

Runnel, P., Pruulmann-Vengerfeldt, P., & Reinsalu, K. (2009). The Estonian Tiger Leap from post-communism to the Information Society: from policy to practice. *Journal of Baltic Studies*, 40 (1), 29-51.

Sæbø, Ø., Rose, J., & Flak, L. S. (2008). The shape of eParticipation: characterizing an emerging research area. *Government Information Quarterly*, 25, 400-428.

Schryen, G. & Rich, E. (2009). Security in large-scale Internet elections: a retrospective analysis of elections in Estonia, The Netherlands, and Switzerland. *IEEE Transactions on Information Forensics and Security*, 4 (4), 729-744.

Simons, B. (2010). *Simons: Internet voting: an idea whose time has NOT come*. Retrieved March 20, 2011, from <[http://microsites.oii.ox.ac.uk/ipp2010/system/files/IPP2010\\_Simons\\_Paper.pdf](http://microsites.oii.ox.ac.uk/ipp2010/system/files/IPP2010_Simons_Paper.pdf)>.

Siseministeerium. (n.d.). *KOV üleminek paberivabale asjaajamisele*. Retrieved March 27, 2011, from <[http://dw.riik.ee/KOV\\_%C3%BCleminek\\_paberivabale\\_asjaajamisele](http://dw.riik.ee/KOV_%C3%BCleminek_paberivabale_asjaajamisele)>.

Streib, G. & Navarro, I. (2006). Citizen demand for interactive e-government: the case of Georgia consumer services. *American Review of Public Administration*, 36 (3), 288-300.

Tallo, I., Ott, A., Leosk, N., Marvet, P., Segaert, S., Trechsel, A. H. et al. (2007). *TOM usage statistics*. Retrieved April 2, 2011, from <<http://tidplus.net/project/analysis-of-the-tom-tool/analysis-of-the-tom-tool-usage-statistics/>>.

The Freedom House. (2011). *Freedom on the Net 2011: a global assessment of Internet and digital media*.

West, D. M. (2004). E-government and the transformation of service delivery and citizen attitudes. *Public Administration Review*, 64 (1), 15-27.

# Recent developments in the transnational information exchange between law enforcement authorities in the EU: The introduction and implementation of the principle of availability

---

---

Konstantia-Christine Lachana

---

---

## 1. Preliminary remarks

The exploitation of personal information as one of the most effective and advantageous means for the implementation of the political and operational activities falling within the realm of the former Title VI TEU is far from being a novelty to the European state of affairs. In this respect, the joint database of the Schengen Information System, one of the most significant countervailing measures against the abolition of EU's internal borders, established by art. 92 of the 1990 Convention implementing the Schengen Agreement<sup>1</sup>, as well as the, initially set up in 1995, computerized system of collected information maintained by Europol<sup>2</sup>, bear clear testimony to the diachronic recognition of the free circulation of personal data as a key tool for the enhancement of police and judicial cooperation in criminal matters, including the transnational cooperation through the EU's coordinating institutions and networks of penal repression. In turn, the said cooperation is steadily perceived as a major prerequisite for the progressive establishment of a European security area, as it is highlighted, among others, in the Presidency Conclusions of the 1999 Tampere European Council<sup>3</sup>.

- 
1. The Schengen *acquis* - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, EEL 239, 22.9.2000, pp. 0019-0062.
  2. Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), EEC 316, 27.11.1995, p. 0002-0032, (art. 6ff.). The Europol Convention has been recently replaced by the Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), EEL 121, 15.5.2009, pp. 0037-0066.
  3. §§40ff., in which a special emphasis is placed on the need to develop common Union-wide, crime-fighting policies, entailing, among others, the stepping-up of transnational cooperation for the repression of all forms of serious organized criminality, with a view to achieving a high level of safety within the AFSJ.

In recent years, however, the terms under which the establishment of this space is being promoted and, by extension, the conditions under which the citizens' supply with a high level of internal security within the EU's area of freedom, security and justice is being ventured seem to have undergone a substantial alteration. The latter is illustrated, among others, by the intensification, -with a remarkable speed and in an exponentially growing number-, of EU concerted law and policy-making efforts towards the expansion of law enforcement authorities' access to an ever increasing volume of personal data on the one hand, as well as towards the abolition of the existent institutional impediments hampering the (pre-Lisbon) third pillar cooperation in data exchange, on the other.

The starting point of the said policy shift traces back to the historic-political concurrence which was configured internationally in the aftermath of the tragic events of September 11<sup>th</sup>. Indeed, with the worldwide, increasing momentum on internal security legislation since 9/11 and the reprioritization of terrorism as a primary security threat, the terrorist attacks on the US are rightfully acknowledged to have impinged as a major catalyst for the formation of the contemporary international, European and national counterterrorist strategies, while accelerating the ongoing transition to a proactively-oriented "globalised system of penal repression"<sup>4</sup>; a system purportedly established in a collective effort to counteract the salient challenges of globalised criminality, especially international terrorism. At EU level in particular, aside from the strong boost that it furnished to the jurisgenerative process and the stream of European integration with respect to Justice and Home Affairs governance in general<sup>5</sup>, the Union's active involvement

---

4. Theoretical conceptualizations of the constitutive elements of the globalised system of penal repression as well as of its' impact on the national criminal civilizations, see among various others on *Albrecht P.-A.* (2003), *Protection of Freedom: Duty of the European development of penal law*, *Günther K.* (2003), *International Crime-fighting Policy: The Evolution Towards a Global Security Law*, both in *Manoledakis I./Prittwitz C.* (Eds.), *Internationalization of Criminal Law*, Sakkoulas publ., pp. 199ff. and 19ff. respectively. Cf. likewise *Günther K.* (2005), *World Citizens Between Freedom and Security*, *Constellations*, vol. 12, n. 3, pp. 379ff.

5. On the impact of 9/11 terrorist attacks upon the formation of the EU "area of freedom, security and justice", see identically *Monar J.* (2002), *The Area of Freedom, Security and Justice After 11<sup>th</sup> September 2001: Problems of Balance and the Challenge of Enlargement*, in *Xuereb P.* (Ed.), *The Future of the European Union: Unity in Diversity*, European Documentation and Research Center, University of Malta, Enterprises Group Ltd., pp. 174-210 (184ff.), *Id* (2006), *Cooperation in the Justice and Home Affairs Domain: Characteristics, Constraints and Progress*, *European Integration*, vol. 28, n.5, pp. 495-509, *Id.* (2008), *The European Union as a Collective Actor in the Fight Against Post 9-11 Terrorism: Problems and Prospects of a Primarily Cooperative Approach*, in *Gani M./Mathew P.* (Eds.), *Fresh Perspectives on the "War on Terror"*, ANU E Press, pp. 209-233, *Den Boer M.* (2003), *9/11 and the Europeanisation of Antiterrorism Policy: A Critical Assessment*, *Policy Paper No. 6*, Groupement d' Études et de Recher-

in the “global war on terror” placed cross-border transmission of personal data and granting access to national databases for a number of actors, in the limelight; initially as an opportune, primary vehicle for the effectuation of its’ counterterrorist strategy. Subsequently and at a secondary level, the political instrumentalization of information exchange at the centre of counterterrorist action facilitated its’ upgrading to the main building block of EU’s internal security architecture, currently under construction. At the core of this architecture lies a gigantic system designed to enable the free flow of personal information regulation, within which all security-related data, collected and processed at the national levels, whether pertaining to terrorism or simply relevant to any other form of conventional criminality, will circulate freely and unobstructedly among all security agencies<sup>6</sup>.

In a nutshell, the sobering findings emanating from the rapidly evolving EU legal landscape in the domain under discussion could be summarized by the general observation that national sovereignty over the collection, distribution and manipulation of personal data is being gradually, yet steadily eroded and replaced by an EU-wide right of data use and process. What is more, the significance of those findings grows dramatically in view of the ominous and rather daunting future prospects set forth by the upcoming and already heralded by the Stockholm Program development of a secure and structured *European Information Exchange Model* on the basis of the evaluation of the enacted legal instruments<sup>7</sup>. The com-

---

ches, Notre Europe, *Id* (2006), Fusing the Fragments-Challenges for EU Security Governance on Terrorism, in Mahncke D./Monar J. (Eds.), *International Terrorism: A European Response to a Global Threat?*, 83ff., Norman P. (2006), Governing the Third Pillar: Institutional Development and External Relations in Justice and Home Affairs Before and After September 11 th. in Carr F./Massey A. (Eds.) *Public Policy and the New European Agendas*, Aldershot: Edward Elgar Publishing, pp. 219-232, Berthelet P. (2002), L’impact des événements du 11 Septembre sur la création de l’espace de liberté, de sécurité et de justice, *Cultures & Conflits*, vol. 46 (partie 1 et partie 2).

6. See generally on this process De Busser E. (2007), The Architecture of Data Exchange, RIDP/IRPL, vol. 78, pp. 35ff., (36), Balzacq T. (2008), The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies, JCMS, vol.46, n. 1, pp. 75-100.
7. The Stockholm Programme- An Open and Secure Europe Serving and Protecting Citizens, EEC 115, 4.5.2010, pp. 0001-0038, at 0018. The Stockholm Programme was adopted by the European Council on 10-11 December 2009 based on the *Commission Communication’s: An Area of Freedom, Security and Justice Serving the Citizen*, (COM) 2009, 262 final, 10.6.2009. The latter had already paved the way for the official endorsement of the European Information Exchange Model, by sketching its’ functionality and foundations (at p. 15): “Security in the EU depends on effective mechanisms for exchanging information between national authorities and other European players. To achieve this, the EU must develop a European information model based on a more powerful strategic analysis capacity and better gathering

plexity of such a stocktaking exercise over the current EU legal framework on crime-related data exchange should not be overlooked. Drawing on the input of the binding, normative instruments already in force, begs indeed the understanding over the undeniable fact that the last seven years have witnessed a proliferation of EU-propelled, legal initiatives aiming at the improvement of access to and exchange of personal information among police and judicial authorities within the framework of their transnational cooperation.

To be sure, the intensive shape-up of ever-expanding information sharing normative schemes for security purposes in the EU, covering the entire spectrum of its' former pillar structure, was squarely rooted upon the fresh, even more pressing impetus for further tightening of penal repression measures provided by the Madrid and London bombings, amidst escalating fears over the invisible, deadly threat posed by "home-grown terrorists" in the Old Continent. Unsurprisingly then, the bulk of these legal initiatives revolves mainly around the three guiding axes that were delineated within the *Declaration on Combating Terrorism*, which was adopted by the European Council on March 25<sup>th</sup> 2004<sup>8</sup> and can be classified as follows. First, the enhancement of transnational cooperation among law enforcement authorities through the simplification of data and intelligence exchange procedures on the basis of the *principle of availability*; *secondly*, the maximization of EU databases' effectiveness upon the technical platform forwarded by the newly-coined *principle of interoperability* <sup>9</sup> and *thirdly*, the development of

---

and processing of operational information. This model must take account of existing systems, including those in the customs field, and overcome the challenges of exchanging information with non-member countries" (emphasis on the original). On 20<sup>th</sup> April 2010, the Commission published an Action Plan detailing how the various aspects of the Programme would be implemented: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions- Delivering an Area of Freedom, Security and Justice for Europe's Citizens: Action Plan Implementing the Stockholm Program, COM (2010), 171 final. See analysis of the latter on House of Lords, European Union Committee, 9<sup>th</sup> Report of Session 2010-2011, Implementing the Stockholm Programme: Home Affairs, Report with Evidence.

8. 7906/04, 29.3.2005.

9. Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the Area of Justice and Home Affairs, COM (2005) 597 final, 24.11.2005. For a critical overview, see among others the EDPS' Comments (10.3.2006), *De Hert P./Gutwirth S.*(2006), *Interoperability of Police Databases Within the EU: An Accountable Political Choice?*, IRLCT, vol.20, n.1-2, pp. 21-35 and *Hobbing P.*(2006), *An Analysis of the Commission Communication (COM(2005)597 Final of 24.11.2005) on Improved Effectiveness, Enhanced Interoperability and Synergies among European databases in the Area of Justice and Home Affairs*, Briefing Paper Order Form No IP/C/LIBE/OF/2005-168, CEPS. On the various EU databases already in force



synergies with the *private sector*, with a view to amplifying the access to data gathered and processed therein for the purposes of the prevention, detection and prosecution of serious criminal offenses<sup>10</sup>.

The common denominator as well as the underlying conceptual substratum of all the previously enumerated security-enhancing policies is the principle of availability. Indeed, given the all-encompassing, multifaceted nature of the availability concept, whose manifestations permeate through the other two previously outlined axes, the focal point of the present contribution will consist in shedding some light onto this groundbreaking and yet highly controversial principle. To this end and by narrowing the focus of enquiry onto the historic background preceding the official adoption of the said principle, the second part seeks to segregate the particulars comprising the vague notion of availability, especially vis-à-vis its' conceptual overlap with the similar notion of equivalent access. The emphasis will then shift to the presentation and analysis of the three keynote legal instruments whose promotion was associated, in the relevant discourse and to varying degrees in each case, with the implementation of the availability principle; namely the so-called Swedish initiative, the Prüm Treaty and the Commission Proposal for a Council Framework Decision on the exchange of information under the principle of availability. Drawing upon the critical assessment and interpretative evaluation of the said initiatives while taking into consideration the latest stream of policy-making projects, some more concrete insights are intended to be gleaned, by way of conclusion, into the future prospects of the availability principle as well as its' contribution to the construction of EU's internal security architecture in the post-Stockholm era. In view of these developments no doubt

---

(SIS, Eurodac, CIS, Europol, Eurojust, Joint Situation Centre-SitCen) as well as on the ones that under development (SIS II, VIS) see Geyer F.(2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security & Justice*, challenge, Liberty & Security, Research Paper No.9, May 2008, Mitsilegas V.(2008), *Databases in the Area of Freedom, Security & Justice*, in Stefanou C./ Xanthaki H. (Eds.), *Towards a European Criminal Record*, CUP, pp. 311-335 and Preuss-Lausinotte S.(2007), *Bases de données personnelles et politiques de sécurité: une protection illusoire?*, *Cultures & Conflits*, vol. 64.

10. The synergies with the private sector were unfolded in two directions, namely the *air transport sector* (cf. PNR data transfer to non-EU countries as well as, most recently, within the EU) and the *telecommunications' sector* (cf. EU Data Retention Directive). For the fact that upon these three axes (availability, interoperability, access to the private sector data) were premised all the legal initiatives in force regarding information exchange for law enforcement purposes, see esp. De Biolley S.(2006), *Collecte, échange et protection des données dans la coopération en matière pénale*, JTDE, 131, pp. 193-199 (194 et seq.) On the multifaceted nature of the availability concept, see also the Common position of the European Data protection Authorities on the use of the concept of availability in law enforcement, adopted on May 11<sup>th</sup> 2007 during their spring conference in Cyprus, p. 6.

can be cast on the fact that striking the appropriate balance between the protection and the exploitation of personal information is the biggest, most challenging and crucial hurdle to overcome.

## 2. Defining availability: the transition from the principle of equivalent access to the principle of availability

In response to the request forwarded by the European Council in the aforementioned Declaration on Combating Terrorism, with regards to the “simplification of information and intelligence between law enforcement authorities of the Member States”, the European Commission presented three months later a “Communication to the Council and the European Parliament towards Enhancing Access to Information by Law-Enforcement Agencies (EU Information Policy)”<sup>11</sup>. At the heart of the Commission’s interest lies the improvement of access to all necessary and relevant data, information and intelligence by all EU law enforcement and security agencies “in order to prevent and combat terrorism, other forms of serious or organized crime as well as the threats caused by them”. This improvement is in turn described as one of the two building blocks of the *EU Information Policy for Law Enforcement*.<sup>12</sup> In setting out the policy goals and strategic objectives to be achieved, the Commission announced the creation of a free market for law enforcement information and criminal intelligence, which will be “open” to hundreds of law enforcement officers and security agencies in the EU, including Europol and Eurojust. Moreover, the critical aim of free data circulation within the European space as well as the production and use of high quality EU criminal intelligence are reckoned, in the Commission’s view, as being attainable through the implementation of the “*principle of equivalent access to data*”. As its’ title suggests, in terms of its’ content, the latter entails the reciprocal obligation to grant

---

11. (COM) 2004 429 final, 16.6.2004. Analysis of the Communication’s content see esp. on Becker S. (2005), Increased Cooperation Between Law Enforcement and Intelligence Agencies After September 11, 2001, RIDP/IRPL, vol. 76, pp. 57-74 (68ff.) and House of Lords, European Union Committee, 5<sup>th</sup> Report of Session 2004-2005, *After Madrid: The EU’s Response to Terrorism*, Report with Evidence, 10.

12. The EU Information Policy’s second building block/core objective regarded the development of EU intelligence-led law enforcement, to be implemented upon the operational platform of a European Criminal Intelligence Model (ECIM) (p. 10ff.), see on this, Council Conclusions on Intelligence-led Policing and the Development of the Organised Crime Threat Assessment (OCTA), 10180/4/05 CRIMORG 56 ENFOPOL 75 as well as Nunzi A. (2007), Exchange of Information and Intelligence Among Law Enforcement Authorities-A European Union Perspective, RIDP/IRPL, vol. 78, pp. 143-151, (147) and Brady H. (2008), Europol and the European Criminal Intelligence Model: A Non-state Response to Organised Crime, *Policing*, vol. 2, n. 1, pp. 103-109.

equivalent rights of access to data and databases to law enforcement officials of other Member States (hereinafter: MS), *under the same or at least comparable conditions* applicable to national law enforcement agencies (p.7).

The assumption of the EU Council's Presidency by the Netherlands a few months later gave way to a new round of negotiations on an entirely new conceptual basis, upon which the central notion of "equivalence" was superseded by the allegedly more operational term "availability"<sup>13</sup>; and as such it was officially integrated in the multiannual *Hague Program*<sup>14</sup>. Specifically, under the headline "strengthening security" and embarking on the conviction that the abolishment of MS' national borders should extend to the flow of law enforcement information, so as "the mere fact that information crosses borders should no longer be relevant", the highest political declaration adopted by the European Council in November 2004, inaugurated an "innovative approach" in the field under discussion, premised upon the "principle of availability"<sup>15</sup>. Within the Program's context no specific mechanism for the exchange of law enforcement information under the principle of availability is foreseen, only the intended outcome of its' application, namely that "with effect from January 1<sup>st</sup> 2008 a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigation in that State".

Comparatively examined, the two approaches in question (i.e. the Commission's and the Council's) bear a strong resemblance to each other, in the sense that they both place a barrier onto the repressive authorities of a MS's discretion to simply ignore a demand from their foreign counterparts if the requested piece of information is available to their national competent authorities. In a similar vein, therefore, and to the extent that they impose an obligation to make the data available to foreign law enforcement authorities for the purposes of the ongoing investigation in *that* State, they equally redound on a strike against national sovereignty, while changing at the same time the terms of the "ownership" status over the collected personal data<sup>16</sup>.

---

13. See the Presidency Note of September 2004 having as a subject the exchange of information (12680/04), at 2.

14. The Hague Programme: Strengthening Freedom, Security and Justice in the European Union, EEC 53, 3.3.2005, pp. 0001-0014.

15. Ibid, at 0007.

16. The fundamental modification of the "ownership" status over the gathered information as a result of the availability principle's implementation is ascertained by a number of theoriti-

The distinguishing feature between the two accounts rests, nevertheless, onto the *degree* of the said intervention in national sovereignty. By all means, the exchange of information under the principle of equivalent access allows for national treatment of requests for information on conditions that are *not stricter* than those applicable to the requested MS. It involves an *indirect* access to personal data held by the competent law enforcement authorities following the submission of a specific request; the former is granted on condition that the national rules governing the procedure of access of the requested State are respected. Differently put, the notion of “equivalence” signifies *precisely* the obligation to ensure *the same* (not stricter) conditions and terms of access which are generally applicable to national repressive authorities of the requested MS pursuant to its’ internal legislation and in compliance with the safeguards already in place therein<sup>17</sup>.

The Dutch-inspired notion of “availability” on the other hand, does not necessarily imply the determination of “equivalence” as was previously construed, taking into account that no such obligation of compliance with the national legislation of the MS in possession of the data is set by the Hague Program. Concomitantly, “equivalence” is merely encapsulated in “availability” as one of its’ less intervening subsets, according to the clarification that was later brought to light by a Presidency’s Note<sup>18</sup>. To be sure, the underlying rationale behind the “simple” in its’ conception principle of availability consists in the imperative for the necessary information to be exchanged “as swiftly and easily as possible between the

---

cians, see e.g. Balzacq T./Carrera S. (2006), The Hague Programme: The Long Road to Freedom, Security and Justice, in Balzacq T./Carrera S. (Eds.), *Security versus Freedom? A Challenge for Europe’s Future*, Ashgate Publ., pp. 1ff and Bigo D. et als. (2007), The Principle of Information Availability, Challenge, available online at <http://www.libertysecurity.org>. The loss of control and ownership goes hand in hand with the deprivation of sovereignty and autonomy, which explains perfectly well the disinclination of security officials towards the centralized mechanisms that are employed in the more integrated data-exchange models, implementing the principle of availability, see likewise esp. McGinley M./Parkes R. (2007), Data Protection in the EU’s Internal Security Cooperation- Fundamental Rights vs. Effective Cooperation?, *SWP Research Paper*, available online at: [http://www.swp-berlin.org/fileadmin/contents/products/research\\_papers/2007\\_RP05\\_pks\\_mcginley\\_ks.pdf](http://www.swp-berlin.org/fileadmin/contents/products/research_papers/2007_RP05_pks_mcginley_ks.pdf).

17. Cf. on the point the remarks made by the Director General of the EU Commission’s JHA’s Directorate General, Jonathan Faull, during his examination as a witness before the House of Lords’ European Union Committee (After Madrid..., *ibid.*, at 38-39), who concludes that “[...] the notion of equivalence means that the national rules of access would have to be complied with in each case”.
18. 7641/05, 25.3.2005, under the subject of: “Approach for the Implementation of the Principle of Availability”, at 3- 4, where equivalent access is presented as the least invasive (and thus, by extension, least effective) modality for implementing the availability principle.

MS' national authorities, preferably by allowing direct online access"<sup>19</sup>. Hence, what was deliberately presented as a simple renaming of the guiding principle underpinning the EU system of data exchange for crime-fighting ends proves to entail in practice a profound transformation of the deep-seated transnational co-operation mechanisms, grounded upon the mutual recognition procedure<sup>20</sup>, with far-reaching *political* and *human rights*' implications. *Political*, insofar as the application of the availability principle compromises the requirements and sustainability of democratic ideals of openness and public accountability and *privacy-eroding* ramifications, to the extent that it calls for sweeping and expedite, free data traffic among national security and police forces across the EU without ensuring appropriate safeguards against "fishing expeditions" or other forms of sensitive information misuse on their part, as it will be further substantiated in the following lines.

### 3. General legislative regime regulating the transnational data exchange: the Swedish initiative

On June 4<sup>th</sup> 2004, that it is to say a few days preceding the submission of the previously cited Commission's Communication and also in fulfillment of the instruction contained in the Declaration on Combating Terrorism, the Kingdom of Sweden tabled an Initiative with a view to adopting a Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, in particular as regards serious offences including terrorist acts.<sup>21</sup> The temporal coincidence between the two proposals is hardly mere form, revealing instead the existence of striking similarities as to their orientation and general philosophy. Chief among them is the application for the first time of the principle of equivalent access by the provisions of the so-called "Swedish initiative"<sup>22</sup>.

The fact that the Swedish initiative is governed by the principle of equivalent access further leads to the detection of all the underlying parameters and elements comprising the said principle within its' proposed mechanism for the enhancement of information-sharing. Hence, to start with, a system of *indirect* access to

19. According to the European Data Protection Supervisor, see his Opinion on the Proposal for a Council Framework Decision on the Exchange of Information Under the Principle of Availability (COM (2005) 490 final), EEC 116, 17.5.2006, pp. 0008-0017, at 0009.

20. On the relation between the principles of availability and mutual recognition see *Mitsilegas V.*(2009), EU Criminal Law, Hart Publ.: Oxford, 257, who characterizes the former as the "maximal version" of the latter.

21. EEC 281, 18.11.2004, pp. 0005-0010.

22. See art. 4§§2 and 3 of the Initiative.

data is instituted following the submission of a specific and directly dispatched by a competent law enforcement authority request, in accordance with the national legislation of the requested State (without prejudice to art. 8 which lays down the conditions for a spontaneous, unasked for, exchange of information). Secondly, an *obligation* to respond “without delay and to the furthest possible extent within the timeframe requested” is imposed, while a time limit of twelve hours at most is set for the provision of information and intelligence on certain types of crimes that are enumerated in article 4a§2. Thirdly, the application of equal and *not more stringent* conditions than those that would apply to a national request on the data access is stipulated.

In terms of its’ objective and scope, article 1 provides that “the purpose of the Framework Decision is to establish rules under which Member States law enforcement authorities may exchange existing information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations”. From this statement it follows seamlessly that the only police activities falling within the regulative ambit of the proposed piece of legislation are those that are conducted reactively, with a view to verifying and identifying the facts, suspects and circumstances regarding one or several, identified as to their commitment, criminal acts, as well as proactively within the framework of a pre-investigation criminal operation during which intelligence is gathered for the purpose of ascertaining the possible or future commitment of concrete punishable behaviors. From a procedural perspective, both police investigation and pre-investigation are effectuated in a pre-trial, pre-evidentiary phase, prior to the beginning of criminal proceedings and even to the decision of whether or not to prosecute. In this direction, article 1§3 explicitly specifies that no obligation to provide information and intelligence to be used before a judicial authority as evidence is implied by the proposed Framework- Decision (hereinafter: F.-D.), nor right to use such information or intelligence for this purpose is founded. In the event of a future, volitional usage of the said information as evidence in a criminal court, the consent of the State which provided the information should be sought beforehand, “where necessary through the use of instruments regarding judicial cooperation in force between Member States”.

With regards to the *types* of the exchangeable information and intelligence, no distinction is drawn to specific data categories. All *existent, directly or indirectly* accessible to the competent law enforcement authorities, criminal intelligence and information are covered, including those held by private entities (art. 2d). Also, the proposed F.-D neither postulates the creation of new national databases nor imposes the obligation to maintain and store “index data”; the decisive criterion being only the accessibility to or existence of sought information or intelligence in the possession of the competent national authority, without any further

engagement encumbering MS to obtain this information by means of coercive measures (art. 1§4).

If all the aforementioned preconditions are met then, in principle and *as a general rule*, the, inaugurated by the Initiative, simplified procedure on data exchange ensues via the communication channels that are set out by article 7. By way of exception, article 11 codifies three classic grounds of data withholding, granting thus the right to refuse the provision of the requested information. The restrictively enumerated cases of refusal are associated with the safeguard of essential security interests of the requested MS, the success of an ongoing investigation or criminal intelligence operation or the safety of the individual, and, finally, the reception of a clearly disproportionate or irrelevant to its' stated purpose, request. *A contrario*, the same right of refusal should be recognised with regards to information on offences of a minor gravity (punishable with a criminal penalty of less than twelve months), as well as to information whose collection presupposes the use of coercive measures, as was previously indicated.

The adoption and enactment of the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union two years later, transformed the Swedish initiative into a legally binding document in the European legal order<sup>23</sup>. The former, although it adheres for the most part to the spirit and guiding principles of the latter, does present certain points of differentiation as well as additions. Indicative in this direction is the elimination of the reference to "terrorist acts" from the title and the, subsequent to this rewording, displacement of the centre of attention to the prevention and suppression of all forms of conventional criminality. Also, non-negligible is the possible inclusion of secret services into the definition of the "competent law enforcement authorities" through the back door and despite the opposite, but non-binding to MS, formulation contained in article 2(a). Finally, another previously non-encountered novelty is the standardization of the procedure for the transmission, delay or refusal of information through the forms that are attached to the two accompanying Annexes.

In the Commission's view, the future dynamics of the Swedish Framework Decision (hereinafter: SFD) are on the increase and the expectations for it to play a growingly significant role within the European Information Exchange Model aim high. Despite the partial, evidence-based feedback on the actual operation of the SFD so far (as a result of its' non-conclusive transposition by all MS) as

---

23. EEL 386, 29.12.2006, pp. 0089-0100. Cf. also the Presidency Note 9512/10 (26.5.2010), containing the Guidelines on the implementation of the "Swedish Framework Decision".

well as the (clearly demonstrated) restricted practical usage of and recourse to the mechanism for the simplification of law enforcement information and intelligence exchange established therein, the Commission, in its' recent Report which was issued pursuant to art. 11§2 SFD<sup>24</sup>, expresses its' confidence that the latter's underlying principles have been implemented at the national legal orders and its' goals overall achieved. In acknowledging that the said legal instrument has not yet reached its' full potential, it is concluded (p.11) that the SFD's usefulness and functional importance are foreseen to be further invigorated, following the enhancement of data exchange in the context of: a) the EU Information Management Strategy (hereinafter: IMS) interoperability coordination project (UMF II) and b) the implementation of the Prüm Decisions (*see infra in text*).

#### **4. Legislative regime regulating the transnational exchange of specific types of information: the Prüm Convention**

On May 27<sup>th</sup> 2005, the signature of the Prüm Convention on the stepping up of cross-border cooperation particularly in combating terrorism, cross-border crime and illegal immigration marked a milestone, trailblazing development in the European transnational information exchange architecture<sup>25</sup>. Signed at the homonym

24. Commission Staff Working Paper, Operation of the Council Framework Decision 2006/960/JHA of 18 December 2006 ("Swedish Initiative"), SEC (2011) 593 final, 13.5.2011. According to art.11§2 SFD, this report was due to be submitted to the Council before the 19<sup>th</sup> of December 2010 and deals exclusively with how the SFD operated practically in the time-frame from December 2008 until December 2010. The assessment of the MS' compliance with the provisions of the SFD falls within the authority of the Council and should be completed no later than the 19<sup>th</sup> of December 2011. The findings of the Commission's report indicate, *inter alia*, that almost two thirds of the MS had transposed the SFD into domestic legislation by the 31<sup>st</sup> of December 2010 (the rest which failed to meet the transposition deadline invoked grounds of lengthy parliamentary procedures- pp. 5-6) and that the majority of the MS which fulfilled this obligation did not draw on the SFD on a regular basis for requesting information because they considered the forms annexed to the SFD to be rather complex and cumbersome (thus they opted instead for an unstructured free-text format- pp. 6 and 10).

25. See the text of the Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration ("Prüm Convention") on the Note 16382/06 of the Council Secretariat (6.12.2006). Critical analysis of the Convention's provisions see identically on Balzacq T. *Et als.* (2006), *Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats*, CEPS Working Document No. 234/January 2006, *Id.* (2006), *The Treaty of Prüm and EC Treaty: Two Competing Models for EU Internal Security, in Security versus Freedom? supra*, 115-136, Balzacq T. (2006), *From a Prüm of 7 to a Prüm of 8 +: What are the Implications?*, Briefing Paper,



German city by the same, seven in number, contracting European States which had concluded the Schengen agreement of 1985 and its' implementing 1990 Convention, and without officially forming part of the Schengen acquis, the Treaty was labelled (not in an approbatory vein, one has to note), as "Schengen III", due to the coincidence in the contracting parties as well as to the identical intergovernmental model of "differentiated integration" upon which it was premised. It consists, in other words, in its' conception a multilateral treaty, which was forwarded outside the ex-third pillar juridical framework, in a deliberate deviation from the latter's inspectional, judicial and parliamentary mechanisms, in order to institute an international conventional regime, binding initially only to its' contracting States. In this regard, these States, impelled by their commitment to "play a pioneering role in establishing the highest possible standard of cooperation especially by means of exchange of information" in the previously enumerated fields<sup>26</sup>, attempted to supplement the, -mainly shaped by the Swedish initiative-, transnational data exchange system for crime-fighting purposes. Notwithstanding the preparatory creation of an "open laboratory" for data transmission in the framework of a "pilot project for cooperation" by the said legal instrument<sup>27</sup>, the ultimate, averred by its' Preamble, goal has been at the outset the incorporation of the Treaty's provisions into the EU legal order. This key objective was achieved three years later, amidst fierce doctrinal criticism, with the enactment of the Council Decision 2008/615/JHA of 23 June 2008 (also known as "Prüm Decision")<sup>28</sup>.

---

IP/C/LIBE/FWC/2005-22, *Guild E./Geyer F.* (2007), *Getting Local: Schengen, Prüm and the Dancing Procession of Echternach- Three Paces Forward and two Back for EU Police and Judicial Cooperation in Criminal Matters*, JECL, vol.1, n.3, pp. 61-66, *Burgess M.* (2007), *The Prüm Process: Playing or Abusing the System?*, ISIS Europe, ESR, n.34, available online at <http://www.isis-europe.org>, *Dehousse F./Sifflet D.* (2006), *Les nouvelles perspectives de la coopération de Schengen: Le traité de Prüm*, *Studia Diplomatica*, vol. LIX, n. 2, pp. 199ff., *Quillet N.* (2007), *Le traité de Prüm relatif à l' approfondissement de la coopération transfrontalière*, RMCUE, n. 513, pp. 660 ff., and *Luif P.* (2007), *The Treaty of Prüm: A Replay of Schengen?* Paper presented at the 10th Biennial International Conference of the European Union Studies Association, held in Montreal on May 17-19 May 2007.

26. As stipulated within the Preamble of the Convention.

27. According to the characterization that was attributed to the Convention by the Luxembourgish Minister of Justice, Treasury and Budget, *Luc Frieden* during his speech entitled: "A New Ambition for Justice and Europe" given in Connecticut, USA, on 1.7.2006, available online at: <http://www.mj.public.lu/ministere/ministre/2006/07/shu/index.html>.

28. Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, EEL 210, 6.8.2008, pp. 0001-0011. In the same meeting and date, two other Decisions have been approved by the Council and published in the OJ with a view to implementing and specifying the Prüm Decision's content; namely the Council Decision 2008/616/JHA of 23 June 2008 on

Comparatively juxtaposed to the Swedish initiative, the Prüm Convention appears to be *in part of a narrower regulatory ambit*, as it does not cover all categories of personal information but it is restricted only to *three* types of them (namely DNA profiles, dactyloscopic data and vehicle registration data) and *in part of a wider reglementary scope*, given that it is not oriented towards the intensification of transnational law enforcement cooperation only through data exchange but it contains *additional regulations* as well, for the stepping up of the *operational* side of the said cooperation, through, for instance, the introduction of joint patrols and operations, the provision of mutual assistance for the prevention of criminal offences in connection with mass gatherings and similar major events, disasters and serious accidents etc. (chap.5, articles 17 *et seq.*)

Furthermore, in terms of the degree of the availability principle's elaboration, the "Prüm model", combines a mixture of modalities of reciprocal access, by means of constructing new national (but not European or central) databases (introducing thus, indeed, from this perspective, an intermediary, "*cautious, gradual, data field-by-data field approach*"<sup>29</sup>, slightly more advanced than the relatively simple system of equivalent access pursued by the Swedish initiative). Specifically and under the general presupposition that the conduct of automated searches will be allowed only in specific cases and in compliance with the requesting MS's national law (*forum regit actum principle*) while taking into account the mutual assistance procedures, *direct* online access is foreseen only with regards to the *vehicle registration data*, that is to say, data relating to owners or operators as well as data referring to vehicles. Conversely, the supply of data falling within the other two categories is subject to the rule of *indirect access* which is afforded to the

---

the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, EEL 210, 6.8.2008, pp. 0012-0072 and the Council Decision 2008/617/JHA of 23 June 2008 on the improvement of cooperation between the special intervention units of the Member States of the European Union in crisis situations, EEL 210, 6.8.2008, pp., 0073- 0075. On the highly interesting background which preceded the Prüm Decision's integration into the EU normative framework (on the initiative of the Federal Republic of Germany) see among many others the two Opinions that were issued by the EDPS (EEC 169, 21.7.2007, p. 7 and EEC 89, 10.4.2008, p. 1 respectively), as well as the analyses which are included in *House of Lords*, European Union Committee, 18<sup>th</sup> Report of Session 2006-2007, *Prüm: An Effective Weapon Against Terrorism and Crime?* 9.5.2007, Kierkegaard S. (2008), *Security and DNA Transfer Within the EU. The Prüm Decision- An Uncontrolled Fishing Expedition in "Big Brother" Europe*, CLSR, vol. 24, pp. 243-252, *Id.* (2010), *DNA Data Exchange: Germany Flexed its Muscle*, in Gutwirth *et als* (Eds.), *Data Protection in a Profled World*, Springer, 227 ff, Guild E. (2007), *Merging Security from the Two-Level Game: Inserting the Treaty of Prüm into EU Law?*, CEPS Policy Brief, n. 124, 22 March 2007.

29. See likewise on the above, first Opinion of the EDPS of July 21<sup>st</sup> 2007, §26, p. 5.

designated national contact points, *initially* only to unidentified, non-attributable directly to any individual, reference data (art. 2§§2, 8 respectively). Aiming at the restriction of foreign authorities' access to the most sensitive types of data, namely the biometric ones, this distinction is rightfully seen as paying due respect to the need for a differentiated legal treatment of personal information according to its' nature<sup>30</sup>.

To be more precise, the said *indirect* access to the national DNA analysis files, as well as to the automated fingerprint identification systems administered by a MS is effectuated on the basis of a *hit/no hit* system, enabling the graduated knowledge over the items sought-for, as follows. At a first level, only the anonymous *reference data* (containing identified or unidentified DNA profiles established from the non-coding part of DNA and a reference number or the dactyloscopic data and a reference number, respectively) are rendered available to the requesting competent law enforcement authorities, for the conduct of searches and comparisons with a view to investigating criminal offences (articles 3§1, 4§1 for the DNA profiles and 9§1 for the dactyloscopic data). In the event of a clear match during the automated searching procedure ("*hit*"), additional information relating to the reference data is furnished through the mutual assistance procedures (including those established by the SFD -articles 3§2, 4§2 in conjunction with art. 5 and art. 9§2 respectively). In the opposite case of a fruitless search ("*no-hit*") the requesting authority is equally notified through automated means (see art. 3§2 *in fine* which applies *mutatis mutandis* to the dactyloscopic data as well). With respect to genetic data in particular, MS are encumbered with the obligation to open and keep DNA analysis files, therefore setting up new databases in this direction (art. 2§1a), on the one hand, as well as to provide legal assistance to their counterparts in the course of ongoing investigations or criminal proceedings by collecting and examining cellular materials regarding a particular individual, present within the requesting MS's territory, in the absence of his DNA profile from the national files (art. 7), on the other.

The previously outlined procedure of automated transfer of specific data types aside, the body of the Council Decision's provisions is complemented also by stipulations regulating the terms of the preventive supply of personal as well as non-personal information (even without the prior submission of a request) in light of upcoming major events with a cross-border dimension, especially sporting events or EU Summits (chapter 3), provisions for the supply of information in order to prevent terrorist offences (chapter 4), the stepping up of the operational aspect of police cooperation (chapter 5), and finally, data protection rules (chapter 6)<sup>31</sup>.

---

30. EDPS, *ibid.*, §80 who applauds the said distinction.

31. According to art. 36§4, the Prüm Decision is due to be evaluated by July 28<sup>th</sup> 2012.

## 5. A highly ambitious and yet unaccomplished, till present, undertaking in view of implementing the principle of availability: the EU Commission Proposal

As anticipated, the active promotion of these legislative initiatives in the time-span intermediating the publication of the Hague Program, boosted the Commission's law-making plans and culminated in the deposition of the latter's own Proposal in December 2005<sup>32</sup>. Interestingly enough, in the official discourse, the degree of the said influence upon the jurisgenerative mobilization of the Union's executive organ is not fully clarified, but it is stressed instead the Commission's intention to bring forward "an entire new concept", much more audacious and devoid of the drawbacks inherent in the other two legislative attempts<sup>33</sup>.

This intention is further corroborated and substantiated by the text of the proposed piece of legislation, whose essence sums up in the, enshrined in art. 6, MS' obligation to ensure that *law enforcement information*, (i.e. information able to make possible, facilitate or accelerate the prevention, detection or investigation of criminal offences, controlled by authorities or by private parties designated for this purpose), is shared with equivalent competent authorities of other MS if they need the information to carry out their lawful tasks, as well as with Europol insofar as Europol's access to the information is necessary for the performance of its' legitimate tasks and complies with Europol Convention and its' Protocols.

---

32. Proposal for a Council Framework-Decision on the exchange of information under the principle of availability, COM (2005) 490 final, 12.10.2005. Analysis of the Proposal's content see esp. on Vermeulen G. et als. (2005), *Availability of Law Enforcement Information in the EU: Between Mutual Recognition and Equivalent Rights of Access*, Maklu, pp. 24 et. seq.

33. Aside from the Swedish Initiative and the Prüm Convention, the Commission put forth a critical evaluation of all the existing legal provisions which fall within the regulative ambit of its' own Proposal, such as the Convention implementing the Schengen Agreement of 1990 and the Europol Convention of 1995 along with its' Protocols. Following this comparative overview and the tracing of similarities among the said provisions, the conclusion which is drawn is in favour of the supremacy of the proposed piece of legislation, see likewise in the Explanatory Memorandum of the aforementioned Proposal as well as in the MEMO/05/367, 12.10.2005, entitled: Proposal for a Framework Decision on Exchange of Information Under the Principle of Availability at 2: "Although today's Commission proposal takes into account important legal developments in the field (Schengen, Europol Convention, Swedish proposal, Prüm Treaty) and benefits from the experience and knowledge acquired with these instruments, it entails an innovative approach so that the objective set out in the Hague Programme becomes true – the mere fact that information crosses borders should no longer be relevant. In this sense, the Commission proposal does not follow a model but intends to introduce an entire new concept." (Emphasis on the original).

Delving into the Proposal's scope of application, which can be inferred by the combination of articles 2, 1§1 and 3a respectively and drawing a parallel between the above and the tantamount one of the Prüm Convention, one cannot but acknowledge a substantial amplification of the existent, available and exchangeable data categories. Indeed, in addition to the three well known types of information, ballistics, telephone numbers and other communications data, minimum data for the identification of persons contained in civil registers are also included<sup>34</sup>. Moreover, no further *subjective* or *objective* criterion is set for the evaluation of the exchangeable information. Hence, the capacity of the data subjects remains indifferent for the application of the Proposal's provisions, which are, by extension, valid indiscriminately for suspects or not for the perpetration of criminally prohibited acts, witnesses, condemned or acquitted persons. In the same vein, no specification is met with regards to the type or gravity of the, encompassed by the Proposal's regulations, criminal acts. The sole restriction that is placed in this direction is of a *temporal* character, given the clarification contained in art. 2§1 that subject to transnational exchange is the information which is processed prior to the commencement of a prosecution. Of a *teleological*, yet equally limiting nature is finally the proviso stipulated by article 7, which constrains the use of the information exclusively to the prevention, detection or investigation of the criminal offence for which it is supplied.

These elements together lead to the assertion that *all* police data as well as *all* data obtained and collected by private enterprises that are accessible to law enforcement authorities for the purposes of the prevention, detection, prosecution etc. of an unlawful criminal conduct fall within the Proposal's ambit. This extraordinary expansion is further aggravated, becoming thus even more problematic, if combined with the observed absence of a distinction regarding the access terms to data. Indeed, unlike the Prüm Convention's formulations, in the case of the Commission's Proposal, the same conditions and modalities are set for all data types. Furthermore and more importantly so, the latter distances itself clearly from the, vital within the aforementioned model, idea of access through a designated national contact point, enlarges the notion of the "competent authorities" and partly reverses the system of progressive and controlled access by yielding priority to the *direct* online access of the equivalent national authorities to all information that is available via electronic, interconnected databases to the corresponding competent authorities of the MS, which is in possession of the relevant information (article 9).

---

34. See detailed enumeration of the types of information that may be obtained under the proposed Decision in order to prevent, detect or investigate criminal offences on the Annexe II of the Proposal, p. 26, to which art. 1§1 and 3 a) refer.

The *indirect* access is assured, in this case, at a *subsidiary* level, that is to say only in the absence of electronically available information. It is effectuated, specifically, through the supply of *index data* (containing at least a reference to the type of information to which it relates as well as to the designated authority in control or handling of that information) for online consultation. The latter entails, as it is also indicated by article 10, the establishment of the appropriate technical infrastructure. The procedure to be pursued relies once again upon the previously outlined *hit/no hit* system, which is complemented here by the additional obligation of transfer of the, incorporated within the “information demand” and identified by the index data, personal information, following the ascertainment of a clear match between the requested information and index data (art. 11). Relying on these pronouncements, one can validly deduce that the Proposal’s central orientation to the provision of *direct* and *widespread* online access (which, as previously recounted, constitutes the prescribed modality for research and consultation only with regards to vehicle registration data in the context of the Prüm Convention), in lieu of their more cautious and graduated communication, reflects a major differentiation in the objectives of the two texts under discussion, with the Commission’s Proposal being the most far-reaching legislative attempt towards the implementation of the availability principle.

To sum up and using as a yardstick the Prüm mechanism, which is a relatively reasonably and moderately deployed mechanism for the upgrading of the cross-border cooperation in the field of transnational exchange of law enforcement information, the “principle of availability” as it is construed and applied by the Commission Proposal aims at the virtual abolishment of national borders with regards to personal information of a criminal interest; at the establishment of a single, EU-wide *modus operandi*, while assuming as already accomplished the necessary high level of mutual trust among national authorities<sup>35</sup>. In theory, it enables the rapid, coherent, homogenous and unobstructed flow of personal information within the European AFSJ, reducing, among others, the uncertainty as to the existence of the requested information. In practice, however, it implies extensive and large-scale reforms to the system of transnational data exchange, entailing on the one hand the loss of sovereignty control over the further course of data processing as well as disproportionate operational and technical expenditure, which has been already alluded to. Considering these consequences and implications, the reluctance of the Council’s Members to enact the Proposal, which remains, until present, at “the level of a

---

35. See on this point the critical remarks of *Piget I.* (2006), *Le principe de disponibilité des informations dans l’espace de liberté, de sécurité et de justice*, in *Bot Y. et al.* (Eds.), *Mélanges à l’honneur de Philippe Léger: Le Droit à la mesure de l’homme*, Paris, Pedone, pp. 257-266 (261).

hopeful monstrosity”<sup>36</sup>, comes hardly as a surprise. By the same token, equally understandable is the Council’s preference towards the Prüm model (a model, which, once again, seems to rely on a more flexible, pragmatic interconnection of existing and expected databases) as the most suitable regulative platform for the implementation of the availability principle<sup>37</sup>.

## 6. The way ahead: towards a European Information Exchange Model- What role for the fundamental rights’ protection?

At present, the negotiations over the adoption of the 2005 Commission Proposal have reached a stalemate and have “frozen” indefinitely, and yet, be that as it may, the highly dynamic prospects of the availability principle within the so-called incubating “European state”<sup>38</sup> can neither be undermined nor outflanked. In fact, ever since the conclusion of the Information Management Strategy (IMS) for EU Internal Security was announced by the Council and Commission Action Plan

36. See Hempel L. et als. (2009), *Exchange of Information and Data Between Law Enforcement Agencies Within the European Union*, Discussion Paper Nr. 29/09, ZTG Themenschwerpunkt: Genese und Gestaltung von Innovativität, Zentrum Technik und Gesellschaft, Technische Universität Berlin, 34.

37. Cf. however on this point the critical reflections of Fuster G./Gutwirth S./De Hert P.(2009), *Analysis of the Value Dimensions of European Law Relevant to Current and Anticipated Challenges of the Internal/External Security Continuum*, INEX DP2, D.2.2., available online at: <http://www.inexproject.eu>, at 7, who argue against the allegedly restricted intrusiveness and the downsizing of the Prüm model’s far-reaching implications: “[A]lthough this latter model could seem to interfere less with national realities, thus not imposing any particular data processing practice, in reality it has had the effect of pushing all participating Member States towards the reinforcement of such processing practices and even towards the creation of new databases, indirectly encouraging all Member States to attain levels of data collection and processing equivalent to those of the Member States more advanced in this field.”

38. In recent years and especially following the adoption of the Treaty of Lisbon and the presentation of the Stockholm Programme, the creation of a “European state” is being exhibited as predestinate. See, e.g. Bunyan T. (2007), *Statewatch analysis- EU: Cementing the European state-New Emphasis on Internal Security and Operational Cooperation at EU level*, *Statewatch Bulletin*, vol.17, n. 3/4, who propounds this theory by corroborating it upon the fact that only a state can apply an internal security strategy. “The introduction of COSI, EU-wide internal security agency cooperation and the European External Action Service are classic instances of EU “statebuilding”- of which there are more examples in the new Title IV on judicial and police cooperation (and immigration and asylum). “State-building” is taken to mean both the creation of bodies and agencies to act on an EU-wide basis (eg: SIS II, FRONTEX, Europol, Eurojust, European Gendarmerie etc) and where administrative (Article 67 covering the whole of former Title IV)) and operational cooperation is centrally organized by the EU (eg: police cooperation, Article 69.i & j)”.

Implementing the Hague Programme<sup>39</sup>, it became clear that the development of such a strategy would essentially serve the purpose of reinforcing, materializing and maximizing the objectives enshrined in the availability principle while building upon its ideological value as a means to further enhance cross-border data exchange cooperation for security purposes. In several instances and by numerous actors the need to remedy the current situation of an “uncoordinated and incoherent palette of information systems and instruments” which “have incurred costs and delays detrimental to operational work” was highlighted and came increasingly to the fore, along with suggestions reaching thus far as the introduction of a “holistic objective in law enforcement information management”<sup>40</sup>.

Capitalizing on the possible benefits stemming from the availability of *all* law enforcement information and intelligence among *all* national and European repressive authorities and security agencies and with a view to boosting the operational cooperation among these agencies, the Council, during its’ meeting of 24<sup>th</sup> October 2008, proclaimed the *principle of convergence*, as “the guiding principle for the continued construction of the common European area of security”<sup>41</sup>. The latter’s (audacious) implementation would entail the reinforcement of the interoperability of EU information systems and by extension their integral and unmitigated compatibility so as to enable the direct online and indiscriminate accessibility to *all* data and criminal intelligence by *all* law enforcement and security agencies<sup>42</sup>.

---

39. EEC 198, 12.8.2005, pp. 0001-0022. See point 3.1 (k), p. 0011, which calls for a “definition of a policy for a coherent approach on the development of information technology to support the collection, storage, analysis and exchange of information”.

40. See *inter alia* the Report of the Informal High-Level Advisory Group on the Future of European Home Affairs Policy (“The Future Group”) entitled: “Freedom, Security, Privacy- European Home Affairs in an open world”, which is attached to the 11657/08 Presidency Note (9.7.2008), §§140ff. (p. 66) in which it is recommended “for the post-Hague Programme that: a) the principle of availability be carried over to a new programme with necessary adjustments and additions and b) an EU JLS Information Management Strategy (EU IMS) be established, with a view to making the principle of availability tangible and providing a coordinated and coherent approach to the exchange of information, aiming at a professional, business-oriented and cost-effective use of information technology and information networks.”

41. Council Conclusions on the principle of convergence and the structuring of internal security, 2899th justice and home affairs Council meeting, Luxembourg, 24 October 2008.

42. See esp. Bunyan T.(2009), *The Shape of Things to Come-EU Future Group*, Statewatch Analysis, available online at: <http://www.statewatch.org/analyses/the-shape-of-things-to-come.pdf>, at 54.



About a year later, the formal adoption of the IMS by the JHA Council concretized how the long-envisioned “EU master plan for information exchange”<sup>43</sup> would be effectuated: through the “streamlining and professionalization of the information management, including the collection, storage, processing, analysis and exchange”<sup>44</sup>. Slightly lowering the level of expectations to a more moderate degree and *anchored again firmly on the methodological premise of the availability principle*, the inaugurated *EU Information Management Strategy* neither endorsed the creation of links between the various databases nor postulated the enactment of new legislative initiatives, “considering the panoply of existing instruments for cross-border information exchange”. It “merely” called for improvement of data-handling in the facilitation of effective data exchange between national authorities and other “European players”, while promoting a “business-driven, efficient and cost-effective development”<sup>45</sup>. The notion of such a “business-driven development” was defined shortly afterwards by the *Stockholm Programme* itself, as encompassing a “development of information exchange and its’ tools that is driven by law enforcement needs”<sup>46</sup>. In outlining the priorities to be addressed within the EU AFSJ for the period 2010-2014, the new five-year plan which was drawn by the Swedish EU Presidency and superseded the Hague Programme, under the

---

43. Council of the European Union, *Note from the Swedish Delegation to Delegations on: Preparing the Stockholm Programme: Conference in Bruges 4-5 March 2009*, 10576/09, 2 June, Brussels, 5.

44. Council Conclusions on an Information Management Strategy for EU Internal Security, 2979<sup>th</sup> justice and home affairs Council Meeting, Brussels, 30 November 2009. As aforementioned (see *supra* ft. 7), prior to the official adoption of the IMS, the EC had also expressed its’ support towards the development of a European Information Model, COM (2009), 262/4, at 15. On the IMS see *inter alia* Töpfer E.(2011), *Lubricating the Flow of Information in the EU*, *Statewatch Journal*, vol. 21, n. 1.

45. As it was specified later on by the EC: “A single, overarching EU information system with multiple purposes would deliver the highest degree of information sharing. Creating such a system would, however, constitutes a gross and illegitimate restriction of individuals’ right to privacy and data protection and poses huge challenges in terms of development and operation [...] The compartmentalised structure of information management that has emerged over recent decades is more conducive to safeguarding citizens’ right to privacy than any centralized alternative”, Communication from the Commission to the European Parliament and the Council, *Overview of Information Management in the Area of Freedom, Security and Justice*, COM (2010) 385 final, 20.7.2010, at 4.

46. *Ibid*, at p. 19. Defined as such, however, this “business-driven development” will essentially grant the repressive authorities the permission to “write themselves wish-lists”, see likewise critically Jones C. (2011), *Statewatch Analysis-Implementing the “Principle of Availability”: The European Criminal Records Information System (ECRIS), The European Police Records Index System (EPRIS), The Information Exchange Platform for Law Enforcement Authorities (IXP)*, available online at <http://www.statewatch.org/analyses/no-145-ecris-epris-ixp.pdf>, at 7.

headline “managing the flow of information”, placed the implementation of the IMS on top of the (reformed, following the entry into force of the Lisbon Treaty) JHA policy agenda, *reiterated the leitmotif role of the availability principle therein* and mandated the EC to “assess the need for developing a European Information Exchange Model based on the evaluation of the current instruments, including the Prüm Decisions and the SFD” (p.18) <sup>47</sup>.

With the necessary legal and political impetus provided for by both the Lisbon Treaty as well the Stockholm Programme, in February 2010, under the auspices of the Spanish Presidency, the long-awaited for *EU Internal Security Strategy* (ISS) was adopted by the Council with a view to setting out a common *European Security Model*.<sup>48</sup> In this vein, the ISS identified a number of principles and strategic guidelines for action as underpinning the elaboration of this Model. Chief among the latter was *on the one hand*, the affirmation of a *proactive (intelligence-led) approach* driven by prevention and anticipation through cross-agency cooperation involving multiple sectors (not just police, judicial and border-management authorities but also the health, social and civil protection agencies)<sup>49</sup> and *on the other*, the strengthening of the existing information and intelligence sharing regimes

47. It is further stipulated that “these assessments will determine these instruments function as originally intended and meet the goals of the Information Management Strategy”. As noted above (ft. 24 and 31) the SFD has already been assessed whereas the assessment of the Prüm Decisions is pending.

48. Draft Internal Security Strategy for the European Union: «Towards a European Security Model», Presidency Note 5842/2/10 REV 2 of February 23<sup>rd</sup> 2010, analysed among others by *Bunyan T.* (2010), First Thoughts on the EU's Internal Security Strategy, *Statewatch Journal*, vol. 20, n. 2 and *Monar J.* (2009), The EU and Internal Security: Origins, Progress, Limits and Prospects of a Growing Role, Real Instituto Elcano (ARI), 112/2009, available at: <http://www.realinstitutoelcano.org>. In November 2010, the Commission tabled a Communication entitled: “*The EU Internal Security in Action: Five Steps Towards a More Secure Europe*”, COM (2010), 673 final, 22.11.2010, where it identified the “most urgent challenges to EU security in the years to come” and proposed a shared agenda of five common strategic objectives and specific actions for the implementation of the ISS between 2011 and 2014, see critical evaluation of the Communication on the Opinion of the EDPS (EEC 101, 1.4.2011, p. 0006-00013) as well as on *Guild E./Carrera S.* (2011), Towards an Internal (In)security Strategy for the EU?, *CEPS Paper in Liberty and Security in Europe*, n.35, available online at the CEPS website.

49. On this proactive, intelligence-led approach which was explicitly mentioned in the Stockholm Programme (along with the focus on the improvement of preventive action) as one of the constituent elements of the ISS (p.18) see esp. *Gruszczak A.* (2010), *Prevention and Anticipation: Pre-crime Approach to EU Internal Security Policy*, Paper presented at SGIR 7th Pan-European Conference *Politics in Hard Times: International Relations Responses to the Financial Crisis*, Stockholm, 9-11 September 2010, available online at: <http://stockholm.sgir.eu/uploads/SGIR2010-Gruszczak-paper.pdf>.

“on a basis of mutual trust and *culminating in the principle of information availability*” (p.13). Once again, special emphasis was laid on the need to employ the IMS with a view to developing a *secure and structured European Information Exchange Model (EIXM)*, which, as it was further clarified “will include *all* the different EU databases relevant for ensuring security in the EU so that there can be interaction between them, as far as it is needed and permitted, for the purpose of providing effective information exchange across the whole of the EU and maximizing the opportunities presented by biometric and other technologies for improving our citizens’ security within a clear framework that also protects their privacy”.

In the framework of defining and eventually enforcing the EIXM which “seeks to *map, assess and recommend* ways to consolidate the cross-border information exchange in the field of EU internal security”<sup>50</sup>, the Commission launched an “information-mapping” project in January 2010 on the legal basis and practical operation (communication channels, information flows and technological solutions) of the exchange of criminal intelligence and information between MS<sup>51</sup>. This stocktaking exercise constituted the first step out of the three, in total, distinctive phases comprising the EIXM exercise (the other two being the assessment of the relevant legal instruments- Prüm Decisions and SFD as well as the elaboration of recommendations on how law enforcement information can be developed in a more efficient and consolidated way). The final results will be presented in the form of a Commission Communication on the EIXM, which is due by the end of 2012<sup>52</sup>.

The layout of the foregoing analysis has vividly illustrated the state of play on the evolution of the availability principle, through which the latter’s predominant, overarching role in the formation of the EU’s law enforcement information and criminal intelligence exchange architecture was corroborated, starting from its’ initial emergence as a manifestation of the key rationale of the Union’s security agenda and *continuum* after 9/11, till its’ recent elevation to one of the ISS’s underpinning cornerstones. Interestingly, at the time of its’ official introduction by the Hague Programme, the principle’s implementation and further elaboration was made, by the EU’s heads of state and government, semi-contingent upon the

---

50. See the Note of the Council’s General Secretariat to the Ad Hoc Group on Information Exchange, entitled: “The European Information Exchange Model”, 5046/10, 6.1.2010.

51. The current draft report of the “information-mapping” project was discussed by experts on April 4<sup>th</sup> 2011 and the final version will be presented to the DAPIX (Working Group on Information Exchange and Data Protection) on May 23<sup>rd</sup> (see the Draft interim Report on the Implementation of the 1st Action List from the Presidency to DAPIX, 8420/11, 15.4.2011, p. 2).

52. Said Communication will follow up the previously mentioned one (see above, ft. 45) entitled: Overview of Information Management in the Area of Freedom, Security and Justice, COM(2010) 385 final (p.28).

strengthening of the (hitherto laden with inconsistencies, deficiencies and shortcomings) AFSJ data protection legal framework<sup>53</sup>, mainly via the enactment of a comprehensive normative instrument to adequately regulate the security-related data processing and erect effective, safeguarding levees against the serious perils emanating from the multitude of privacy-curtailling initiatives which have seen the light. Nevertheless, in spite of its' (belated) adoption, the so-called *Data Protection Framework Decision* 2008/977/JHA of 27<sup>th</sup> November 2008 "*on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*"<sup>54</sup> (DPFD-whose purported aim was, *à propos*, the counterbalance and restriction of the availability principle's ambit, according to the fifth par. of its' Preamble) fell short of aspirations which had envisioned it as the ex-third pillar tantamount legal tool of the EC Directive 95/46/EC; not least because it bore the clear imprint of the lowest -common-denominator agreement.

The latest endeavor towards the establishment of a *harmonised*, consolidated and robust EU-wide data protection regime was initiated by the Commission, which, on November 4<sup>th</sup> 2010 tabled a Communication entitled: "*A comprehensive approach on personal data protection in the European Union*", presenting therein its' perspective on the review of the EU data protection legal system in all areas of the Union's activities<sup>55</sup>. This Communication, whose issuance was prompted *also*

53. For an extensive, overall presentation of these shortcomings and loopholes see among many others De Hert P./Bellanova R.(2009), *Data Protection in the Area of Freedom, Security and Justice: A System Still to Be Fully De-veloped?* Briefing Paper for the LIBE Committee of the European Parliament, available online at: <http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=25213>, De Hert P./Papakonstantinou P./Riehle C. (2007), *Data Protection in the Third Pillar: Cautious pessimism* in Maik M. (Ed.), *Crime, Rights and the EU: The Future of Police and Judicial Cooperation*, JUSTICE publ., pp. 121-194, Alonso Blas D. (2009), *First Pillar and Third Pillar: Need for a Common Approach on Data Protection?* in Gutwirth S. et als. (Eds.), *Reinventing Data Protection?*, Springer, pp. 225-237, O' Neil M. (2010), *The Issue of Data Protection and Data Security in the (Pre-Lisbon) Third Pillar*, JCER, vol. 6, n. 2, pp. 211-235.

54. Council Framework Decision 2008/977/JHA, EEL 350, 30.12.2008, pp. 0060-0071. Analysis and critical assessment of its' provisions see esp. on De Hert P./Papakonstantinou V. (2009), *The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters- A Modest Achievement However Not the Improvement Some Have Hoped for*, CLSR, vol. 25, n.5, pp. 403-414. On the earlier drafts see Kosta E. et als. (2007), *Data Protection in the Third Pillar: In the Aftermath of the ECJ Decision on PNR Data and the Data Retention Directive*, IRLCT, vol.21, n.3, pp. 347-362 (351ff.), De Hert P. et als., *Data Protection...*, *ibid*, 162ff., McGinley M., *Data Protection...*, *supra*, (ft. 16), pp. 14ff.

55. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *A Comprehensive Approach*

by the momentum of the Lisbon Treaty's enactment (*viz.* the standardization of the right to data protection as an autonomous fundamental right and the provision of a direct legal basis for securing it across the entire spectrum of EU competencies by art. 16 TFEU), is intended to be followed this year by a proposal for a new, *general* binding legal instrument. The feasibility of enforcing such a consistent, uniform, identifiable and transnational data protection policy and of promoting "universal principles", along with the Union's commitment to defend its' self-attributed role as a staunch defender of fundamental rights by embedding a true, *common, rights-based culture* among its', shaped by the liberal constitutionalist tradition, Members remain yet to be confirmed.

---

on Personal Data Protection in the European Union, COM (2010) 609 final, 4.11.2010. On January 14<sup>th</sup> 2011 the EDPS released his *Opinion* on the Communication. The latter is retrievable from the Supervisor's website (<http://www.edps.europa.eu/EDPSWEB/>).

# I (do not) consent to behavioural advertising

---

---

Evangelia Mesaikou

---

---

## 1. Introduction

During the last years, the online advertising industry has developed new techniques in order to maximize its benefits by providing more targeted advertisements to internet users according to their interests. By placing cookies or other tracking devices into the users' terminal equipment, advertisers collect data and create a profile for each user based on the web pages visited and the searches made and then provide tailor made advertisements. For example, online advertisers may know or assume your gender, where you live, where your next vacation is planned and even more intimate details, such as if you are trying to lose weight, if you have medical disorders, and they use that information to provide you with advertisements that might interest you. This is called behavioural advertising and it is considered to be the most effective way of online advertising. This is because it helps advertisers to reduce the amount of advertisements shown (and consequently their cost) only to a target of users and at the same time increase the percentage of responses to their advertisements. Internet users can also benefit from behavioural advertising because they will not receive many irrelevant advertisements and they might get to know products that they are interested in (Petty Ross 2000).

However, online behavioural advertising raises some important data protection issues. The most significant problem is that most internet users are not aware that third parties, and not only the sites they visit, install tracking devices to their terminal equipments and can trace their activities and compile profiles for them. In other words, they are not informed who has access to which data and for how long in order to consent or not to this processing.

Since tracking devices are installed in the terminal equipment of the internet user (data subject), and sites access this information in order to process data and build up a profile for the individual, the European framework of data protection legislation is applicable (Directive 95/46/EC and Directive 2002/58/EC, so called e-Privacy Directive). Under these legislations, the advertising network providers and the publishers of the advertisements have specific obligations and the data subjects should be granted with specific rights.

Due to the recent amendment of the e-Privacy Directive, which has to be implemented into national law of the Member States until 25/05/2011, the lawfulness of behavioural advertising has become a flaming issue for academics, regulators and industry. This is because, under the amended version of Article 5(3) of the e-Privacy Directive, the informed and freely given consent of the data subject is a prerequisite for the data processing in order for online behavioural advertising to be lawful. Online behavioural advertising is also at the top of the agenda in the US, where Representative Jackie Speier (D-California) recently introduced the “Do Not Track Me Online” Act, which calls on the Federal Trade Commission (FTC) to issue regulations, requiring that Web companies allow consumers to opt out of online tracking; in addition, Representative Bobby Rush (Illinois) reintroduced an online privacy bill that would require ad networks to obtain users’ consent to tracking. As a response to these regulatory changes, the online advertising industry is trying to come up with solutions (mainly through self-regulation or privacy by design schemes) in order to be compliant with the law without having to restrict the profitable business of targeted advertisements.

This paper is structured as following. The legal requirement of consent to behavioural advertising, under the amended version of Article 5(3) of the e-Privacy Directive, is further analyzed in section 2. Moreover, possible solutions which are proposed in the EU and the US in order to address these data protection concerns are examined in section 3, and, in particular, the default browsers settings, the “Do not Track” lists, the use of a warning icon and the feasibility of opt in mechanisms. Finally, the conclusion of this paper is that a balance should be found in order not to overly restrict behavioural advertising business but at the same time protect the privacy and data protection rights of the internet users. From this perspective, my recommendation is that the default privacy settings should change in order to require affirmative action by the user to consent to be tracked for commercial purposes. Additionally, a layered approach might be the most effective mechanism to provide the users with notice and choice.

## **2. Legal requirement of consent to behavioural advertising**

In order to examine the data protection issues raised in online behavioural advertising, we should understand how it works, the factors involved and the methods used. In online behavioural advertising there are three different roles: the advertising network providers (also referred to as “ad network providers”), the advertisers and the publishers. The ad network providers are the most important factors since they are the ones that connect the advertisers with the publishers. In other words, their role is to display advertisements of their associated advertisers on the specific space reserved for this reason in the publishers’ web pages. In order to be more effective and display the most interesting advertisements to each

user, they use tracking methods so as to identify each internet user as a unique user, collect information for him/her while the user is browsing online and compile his/her profile (Article 29 Data Protection Working Party, 2010). As the network of ad network providers can include hundreds of different web pages, the ad network providers collect a lot of information for each user and can compile a rich profile about his/her activities and interests.

The main tracking method for the purposes of online behavioural advertising is the use of cookies. Other methods, less common and more pervasive while some even illegal, are the use of data mining software and spyware, but these are out of the scope of this paper. Cookies are piece of data that a webpage sends to a web browser, along with a request that the user's web browser retains it. The cookies used in the above scheme of behavioural advertising are third party cookies, because they are placed from a third party (the ad network provider) into the user's browser when the user is visiting a webpage (of a publisher) that contains content from this third party (ad network) provider. Lately, online advertising companies have started using more persistent types of cookies in order to improve their services, such as super cookies and Flash cookies. These are "stronger" cookies because they use mechanisms which are able to store users' identifiers in more persistent way, sometimes recover deleted cookies. These cookies cannot be deleted through the traditional settings of a browsers (ENISA, 2011).

According to ENISA's Report, *"some studies showed that the penetration of the top 10 third-parties grew from 40% in 2005 to 70% in 2008, and to over 70% in September 2009. Another study shows that not only are these third-parties increasing their tracking of users, but that they can now link these traces with identities and personal information via online social networks"*. The protection of users' equipment against this increasing penetration by third parties should be an objective itself. Article 5(3) of the e-Privacy Directive is applicable because of the penetration to the user's equipment, meaning the use of cookies, regardless if the data processed constitutes personal data under the meaning of Directive 95/46/EC. Apart from that, depending on the circumstances and the nature of the processing executed by this penetration, as well as the types of data processed from the users' equipment, the Directive 95/46/EC may apply to such processing. The latter is fully applicable except for the provisions that are specifically addressed in the e-Privacy Directive (Article Article 29 Data Protection Working Party, 2010). Therefore, the principles of data quality, technical and organizational security measures, data retention period, the rights of the data subjects and the protection of sensitive data should be respected as well. For the purpose of this paper, we will focus on the requirement to obtain the users' consent under the amended version of Article 5(3) of the e-Privacy Directive.



Article 5(3) reads as following: *“Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on the condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.”* Therefore, Article 5(3) applies to HTTP cookies, Flash cookies and any similar devices, which may perform the functions described in the provision (EC, Information Society and Media DG, 2010). According to this Article, cookies that are not strictly necessary for the provision of the service requested by the user may only be used if the user has given his freely and informed consent in advance. Under this exception usually fall first party cookies, which are cookies sent by the webpage visited by the user in order to “remember” the preferences of the user, such as the language settings, purchase list, or username and password. However, online behavioural advertising cannot fall under this exception. Even if someone would argue that internet is flourishing and there are many online services free of charge because they are financed by advertisements, therefore, behavioural advertising, as the most profitable way of online advertising, is necessary for the provision of online services and therefore it should fall under this exception, this is not a correct argument. The exception that is covered by the above Article is only for “strictly necessary” processing in order to provide a service explicitly requested by the user, and, thus, behavioural advertising cannot be considered as such and the prior consent of the user is required (EuroPriSe, 2010).

In order for consent to be valid, it should be informed and freely given before the placement of the cookie. The users should be provided with all the relevant information about the cookie and the processing, which should include the identity of the controller, the recipients of the data, the purposes of the processing and any disclosure to third parties. This information must be provided in a user friendly way, so as to be easy for the average internet user to understand to what he/she is about to consent. The user should have the choice to accept or refuse the placement of the cookie and moreover consent should be revocable. This means that any time the user would like to change the settings and revoke his consent about such processing, it should be easy to do it and his/her choice must be respected. Moreover, consent must be specific, which means that any change for the purposes of the processing that is given after the user’s consent (EC, Information Society and Media DG, 2010).

The responsibility to provide such information to the internet user lies with the entity which sends the cookies and retrieves information from the cookies stored on the terminal equipment of the user, thus, most commonly, the ad network providers. In some cases, when publishers are joint-controllers with ad network providers, for example, when they transfer directly identifiable information to ad network providers, they are obliged to provide information to users about the data processing (Article 29 Data Protection Working Party, 2010). Therefore, collaboration is needed between ad network providers and publishers to provide in a user friendly way and in understandable language the necessary information to the users. Moreover, since users usually ignore that third parties might send them cookies when they visit a publisher's webpage, publishers are responsible to inform them (in a user friendly way of course and not in between the long list of terms and conditions of their webpage) that they "rent" place to ad network providers to display advertisements and warn them that these third parties might send cookies to them.

After this short analysis, it is obvious that under the amended version of Article 5(3) of the e-Privacy Directive, the prior informed consent is required before a cookie is sent to the user's terminal equipment and therefore in order for online behavioural advertising to be lawful, the ad network providers should obtain in advance the consent of the internet users to be tracked for the purposes of advertising. Any company operating in the EU market or any online product that is targeted at EU consumers must comply with this rule. This might constitute a problem for many companies after May 25<sup>th</sup> 2011, which is the deadline for the implementation of the amended e-Privacy Directive into national laws. In the next section, the different solutions proposed by industry and regulators to address this issue are presented.

### **3. Technical solutions to obtain consent**

Currently, online behavioural advertising is taking place based on opt out methods. This means that ad network providers send cookies to internet users' terminal equipments in order to process their data and provide them with targeted advertisements unless users have opted out from receiving third party cookies. Article 29 Working Party urges publishers and ad networks to move away from opt-out mechanisms and create prior opt-in mechanisms instead. Users should provide their consent with an affirmative action that shows their "willingness to receive cookies and the subsequent monitoring of their surfing behaviour"; inaction of the users to change their settings does not mean that they consent to be tracked according to the amended Article 5(3) of the e-Privacy Directive. So far, different solutions to address this issue were proposed and some of them are

already implemented through self regulation from some companies. Below is a short analysis of the main mechanisms proposed.

### ***Default settings of internet browsers***

At present, the default settings of web browsers are set to accept first and third party cookies and they give the choice to the internet user to change these default settings and choose either to opt out from receiving third party cookies or to be asked for permission before a cookie is sent to his/her terminal equipment. Under the new requirement of prior consent, the current default settings of the browsers are not sufficient anymore because the user's consent cannot be implied if the user does not change his/her browser's settings. Most of the users are unaware of the fact that not only the sites they visit but also third parties install cookies to their terminal equipment in order to process certain data and they usually also do not know how to change their browser's settings (Article 29 Data Protection Working Party, 2010).

Therefore, the current default settings of the browsers are not compliant with the legal requirement of prior consent. If the default settings didn't have anything to do with would be not to accept third party cookies which would then require ad network providers to obtain the user's consent before the placement of each cookie accepting most probably with a pop up window, they would be compliant with the law but this would not be a user friendly solution. Imagine, while a user is surfing online, a pop up window to appear almost each time the user is visiting a different webpage informing him/her about the cookies and requiring the user's consent. Probably this would have the exact opposite results, by annoying the user who would click "accept" to everything without reading the provided information, just to make the procedure faster and get rid of the pop up window. In addition, it seems that under this setting, users would still be tracked through Flash cookies or other mechanisms.

It seems that the presented solution of browsers' settings is a very unconditional solution, since it offers to the user the choice either to receive all third party cookies or opt out altogether (Berger, 2010). Even if the browsers implement this change into the new versions they release, practically it might take many years for browsers with the old default settings that have not been updated to be phased out, thus rendering ad network providers non-compliant in relation to the browsers outdated to those outdated browsers in the meantime. Therefore, collaboration with browsers and ad network providers is needed in order to find a more suitable solution, which could consist in a combination of default browsers' settings not receiving third party cookies with a good mechanism in place for ad network providers to obtain consent in order to provide their services to the us-

ers. For such mechanism, a layered approach could be a promising solution and this is further analyzed in the conclusions and recommendation section.

### ***“Do not Track” lists***

The solution which is more favourable in the US is the implementation of a mechanism so called “Do not track” lists. The Federal Trade Commission (FTC) in its preliminary staff report, issued in December 2010, proposed a new privacy framework and suggested the implementation of Do not Track lists in order to promote self-regulation in online behavioural advertising. However, the FTC has not endorsed any, “Do not Track” mechanism yet. As a result, it is not clear exactly how this could be implemented, but the most practical method of providing a browser based mechanism would likely consist in placing a setting similar to a persistent cookie on the user’s browser, which would convey that setting to the web pages visited to signal whether or not the consumer wants to be tracked or receive targeted advertisements (FTC Staff Report, 2010).

After the release of the FTC Report, the industry has taken the initiative to develop and even implement such mechanisms through self-regulation. Both Microsoft and Mozilla released new versions of their browsers (Internet Explorer 9 and Firefox 4 respectively) which support a “Do not Track” mechanism. This mechanism is inactive at the default settings of the browsers and the user has to add a list or lists made by organisations or customise his own “Do not Track” list. Such list contains web addresses that the browser will visit/call only if the user visits them directly by clicking on a link or typing their address. By limiting the “calls” to these websites and resources from other web pages, the lists limit the information these other sites can collect. At the moment, ad network providers do not have any legal obligation to abide by these users’ stated preferences, but it is a bit of an honour system and the effectiveness of such mechanism is not yet tested.

Under the requirement of prior opt-in consent set by Article 5(3) of the e-Privacy Directive, the current implementation of such mechanism would not be adequate in the EU, since it is inactive as a default browser setting. Moreover, its effectiveness has yet to be tested and also a more clear definition of what the notion “tracking” includes is needed. If all the tracking methods are banned by the “Do not Track” mechanism and if this is active in the default browsers’ settings, then it might turn to be more effective than the blocking solely of third party cookies.

### ***Warning Icon***

In the US TRUSTe, an internet privacy services provider has launched a pilot program, called Behavioural Advertising Notice and Choice Program, based on the FTC and industry coalition self-regulatory guidelines for behavioural advertising.

Publishers who participate in this pilot program will display the TRUSTe icon and a message (such as “Your Info and Ads”) on their web pages where behavioural advertising takes place. “After the user has clicked on this icon, a pop up widget will open, providing users” with a short notice about the advertisements appearing on the site, the available choices to opt-out and the ability to leave feedback or file a complaint. The pilot will test icon placement, alternative notice and choice messaging as well as consumer engagement levels. Yahoo and Google are participating in this program and they have started using this TRUSTe icon. These companies link the ad icons to tools allowing users to change the categories of interests of their associated companies and to opt out from receiving behavioural advertisements. The large online services companies (i.e. Google, Yahoo, Microsoft, AOL) have decided to use the same icon in order to have a united approach and make it easier for the user to recognize it and understand its use. The icon proposed by TRUSTe is the following:



The use of warning icon is also supported in the EU, such as in the European Advertising Standards Alliance Report (2010), in order to provide in a user friendly way notice to the users about behavioural advertising.

The industry can conduct surveys in order to find the most effective icon and messages icon to attract consumers' attention, without misleading them. Such a survey (Hastak and Culnan, 2010) showed that messages such as “*Why did I get this ad?*” and “*Interest based ads*” had greater interaction with the users than “*Sponsor ads*” or “*Adchoice*”. It would be important as well to adopt the same or a similar icon in order to make it easier for the user to recognize it and understand its role. Land make this approach all the more effective. This approach could bear Fruits; consumer education is however needed to improve the effectiveness of the communication adopted by the ad network providers over time.

### ***Feasibility of opt-in mechanism***

Another proposal is a universal choice mechanism, which would give the users the choice to opt out completely from being tracked and offered targeted advertisements as well as the choice to see the categories of advertising associated with them, de-select some categories and/or select additional ones. Under this approach, users would be able to choose what type of advertisements they are interested to receive or “whether or not they want to” receive targeted advertisements at all.

The feasibility of such mechanism as the universal basis is not yet confirmed by industry. However, some companies, such as Google, already have in place a similar mechanism for their associated companies. Under this mechanism, the so called Ad Preference Managements, the user gets notice of the more or less 20 categories and 600 subcategories that have been associated with the tracking cookie in the user's browser and that gives him the choice to specify which categories he/she is really interested in or, alternatively, it gives him/her the choice to opt-out completely from having his data collected for the purposes of online behavioural advertising (Szoka, 2009). A similar mechanism is used by Yahoo as well.

Such universal mechanism would facilitate the user since he/she would give his choices in "one-shop stop" and not in each company's ad preference mechanism. However, apart from the consent issue, it raises some other issues as well, such as it raises some other issues apart from consent, such as data access and data retention period, security etc. Moreover, since the user's consent needs to be specific, it is doubtful whether consent for tracking for specific categories in such universal mechanism would be sufficient for the processing of data by different companies based on this consent.

#### **4. Conclusion and recommendations**

As it was analysed, online behavioural advertising is a very effective way of advertising and a very profitable business. According to the Interactive Advertising Bureau's Report conducted by the PricewaterhouseCoopers LLP (2010), "Internet advertising revenue in the U.S. totalled \$6.2 billion in the second quarter of 2010, an increase of 4.1 percent from the 2010 first quarter ... and an increase of 13.9 percent from the 2009 second-quarter ... Year-to-date Internet advertising revenues through June 2010 totalled \$12.1 billion, up 11.3 percent from the \$10.9 billion reported for the same six-month period in 2009." However, according to another report conducted by the Ponemon Institute (2010), the online advertising industry is seriously concerned about the data protection issues raised and this has a potential impact on the industries benchmark impact. The survey conducted showed that for the benchmark sample, the average lost potential spending on online behavioural advertising amounts to 6.72\$ million, and the average opportunity loss resulting from privacy concerns is 30.69\$ million.

On the other hand, despite the benefits that online behavioural advertising has for the advertising industry and also for the consumers, the tracking of the consumers/users is taking place most of the times without their knowledge and consent. Internet users ignore the fact that third parties send cookies and track their online behaviour in order to provide them with tailor made advertisements. They

think that what they do online is private and they behave accordingly, for example, they tend to type in search engines very intimate queries, even for their medical problems. An empirical study on how users perceive behavioural advertising showed that 64% of the sample finds the idea of behavioural advertising invasive and that only 51% believes that behavioural advertising is happening a lot now (McDonald and Cranor, 2010).

Therefore, online behavioural advertising needs to change. Under the amended e-Privacy directive, the ad network providers need to adopt another change, which is the requirement to obtain the prior informed consent of the user before the placement of the cookies to his/her terminal equipment, as analyzed in section 2. Member States have to implement this Directive into national law until 25/05/2011; however, regulators and business seem to be quite unprepared for this change. There are no recommendations about the implementation of the Directive into national law issued by any Data Protection Authority to date and at the same time the discussions about technical solutions from the business are still ongoing.

Recognizing that online advertising plays an important role in financing free online services and in fostering internet innovation, it is understandable that a balance should be struck between the conflicting interests of behavioural targeting users and respecting users' privacy and data protection rights. It is immensely, hugely important to find and implement potential solutions to protect users' rights, without going too far and as a result overly restrict the behavioural advertising industry. Since online behavioural tracking and advertising should not take place without the user's consent, business should develop user friendly opt-in mechanisms. At the moment, a layered approach seems to be the most promising solution and such a scheme is shortly presented below.

A layered approach should first of all have different default browsers' settings. Under these default browsers' settings either third party cookies will be rejected unless the user adds specific exceptions or a "Do not Track" list will be activated (if its effectiveness and adequacy is tested). Consequently, the users will not be tracked and offered behavioural advertisements anymore without their knowledge and consent. Needless to say that the users will still be provided with advertisements, but not based on tailor made ones based on profiles compiled for them through tracking. Secondly, the online advertising industry should come up with innovative, user friendly mechanisms to obtain user's consent. It is advisable not to have too many different mechanisms in order party at a place to avoid confusing not to confuse the users. Such mechanisms could be the use of a marketing message users place reserved on the web pages by the publishers for advertisements, inviting the users to visit the webpage of the ad network provider, where there would be information about online behavioural advertising as well as in-

formation about the data controller and the tracking practices of this ad network provider. The user would then be offered the option to consent to be tracked for behavioural advertising by this ad network provider and possibly also to choose some categories he/she would like to receive advertisements for. Therefore, education of the users is needed in order to understand better how internet and the online advertising industry are working. Besides that, each time a behavioural advertisement is shown to the user, the warning icon could be displayed of behavioural advertising, such as the one proposed by TRUSTe, could be displayed on the advertisement in order to provide information to the user why this advertisement is shown to him/her and give him/her the chance to revoke his consent.

Even if the industry seems reluctant to give up the current opt-out mechanisms on which online behavioural advertising is based now, the law in Europe has changed and industry needs to keep up with this change and bring innovative solutions in order to be lawful and at the same time keep the benefits of behavioural advertising. There is a need for greater transparency and better user notice and choice opt-in mechanisms.

## References

Article 29 Data Protection Working Party (2010), Opinion 2/2010 on online behavioural advertising, online at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf) /accessed 31.03.2011

Berger, D. (2010), Balancing consumer privacy with behavioural targeting, online at <http://ssrn.com/abstract=1693029> /accessed 31.03.2011

ENISA (2011), Bittersweet cookies. Some security and privacy considerations, online at <http://www.enisa.europa.eu/act/it/library/pp/cookies/> accessed 31.03.2011

European Commission (EC), Information Society and Media DG (2010), Working Document with subject: Implementation of the revised Framework– Article 5(3) of the ePrivacy Directive, online at: <http://itek.di.dk/SiteCollectionDocuments/Blandet/Sikkerhedsnyhedsbrev/COCOM10-34%20Guidance%20Art%205%283%29%20eprivacy%20Dir.pdf> / accessed 31/03/2011

EuroPrise (2010), Position paper on the impact of the new “Cookie Law” on certifiability of behavioural advertising systems according to EuroPriSe, online at: <https://www.european-privacy-seal.eu/results/Position-Papers/PDF%20-%20EuroPriSe%20position%20paper%20on%20the%20new%20cookie%20law.pdf> / accessed 31/03/2011

FTC Staff Report (2010), Protecting consumer privacy in an era of rapid change, online at: <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf> /accessed 31/03/2011



Hastak, M. and Culnan, M. (2010), Online Behavioral Advertising "Icon" Study, online at: [http://futureofprivacy.org/final\\_report.pdf](http://futureofprivacy.org/final_report.pdf)

McDonald, A. and Cranor, L. (2010), Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising, online at: <http://www.aleecia.com/authors-drafts/tprc-behav-AV.pdf> / accessed 31/03/2011

Petty, Ross D. (2000), Marketing Without Consent: Consumer Choice and Costs, Privacy, and Public Policy. *Journal of Public Policy & Marketing* 19, no. 1: 42-53

Ponemon Institute LLC (2010), Economic impact of privacy on online behavioral advertising. Benchmark study of Internet marketers and advertisers, online at: [http://www.evidon.com/documents/OBA\\_paper.pdf](http://www.evidon.com/documents/OBA_paper.pdf) / accessed 31/03/2011

Price water house Coopers LLP (2010), IAB Internet Advertising Revenue Report, online at: [http://www.iab.net/media/file/IAB\\_report\\_1H\\_2010\\_Final.pdf](http://www.iab.net/media/file/IAB_report_1H_2010_Final.pdf) / accessed 31/03/2011

Szoka B. (2009), Google's Ad Preference Manager: One Small Step for Google, One Giant Leap for Privacy. *The Progress & Freedom of Foundation*, volume 5 issue 2, available online at <http://ssrn.com/abstract=1421876> / accessed 31/03/2011

# RFID in the supply chain and the privacy concerns

---

---

Nikita Maria

---

---

## 1. Introduction

The Radio Frequency Identification Technology (RFID) is an emerging technology that has received considerable attention during its development. RFID dates back in 1948 when it was first used for military applications. Its commercial activities began later in 1960, when electronic article surveillance equipment was developed to counter theft, and in 1970, when laboratories started working on RFID and companies started developing RFID. The 1980s became the decade for full implementation of the RFID technology and in the 1990s widespread use of the technology led to the creation of standards. From 2000 until today, RFID explosion continues and it is believed that over the next years it will experience wide implementation, replacing the barcode technology, which is widely used nowadays.

RFID technology offers powerful benefits to its adopters and today is already being used in a variety of applications, such as payment systems, access control as well as animal and human tracking. Among other applications, RFID is used for a wide variety of supply chain activities too and it seems to be essential for successful supply chains since it plays a key role in order to gain a competitive advantage and differentiate from others.

This paper examines the impact of the RFID technology on the supply chain management. It explains how the technology can be used, the way it influences the management of the supply chain and what are the benefits gained at manufacturing, warehousing, distribution and retailing. Also, it presents the problems that are created specifically at the retail stage where the consumer is involved.

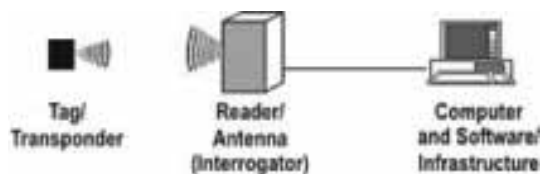
More attention is given to the privacy risks and the legal concerns that arise from the implementation of the RFID technology. While RFID offers great productivity benefits, it also addresses consumer privacy concerns, which result from the lack of current data protection laws. So, in order to be able to see through the privacy concerns that arise from its implementation, it is primary to learn and understand the way the technology works.

In the next chapters, an overview of the main components of the technology is given and the most popular applications are presented. Then, we focus on its implementation to the supply chain and we discuss about the benefits and the

barriers for its adoption. Also, we examine the way American consumers reacted when the RFID technology entered in their personal lives and we present the most recent proposed legislation in several states in the USA. We also discuss about the proposed guidelines in Japan and the activation of the European Union to protect the consumer privacy, providing guidance to the Member States. Finally, some legal proposals and recommendations are made.

## 2. An overview of the RFID technology

A basic RFID system consists of three main components: the RFID tag, the reader and the back-end IT system. The tag is attached to the object and communicates with the reader, using an antenna, which in turn communicates with the enterprise system (Figure 1). Furthermore, the tag is the most important component, as it stores specific information about the object in an analogue form and after the transportation from the tag to the reader using the antenna, the data are retrieved in a digital form from the back-end IT system. Then, the back-end IT system links to a database to obtain more information about that object. Thus, data can be stored both in the tag and the back-end IT system to which the tag refers and be cross-referenced and combined to find out the object's history.



Source: [http://www.aimglobal.org/technologies/RFID/what\\_is\\_rfid.asp](http://www.aimglobal.org/technologies/RFID/what_is_rfid.asp)

Figure 1 A basic RFID system (31)

An RFID tag works as a transponder and consists of a microchip and an antenna. As mentioned previously, the RFID tag communicates with the reader, using an antenna and according to the way it communicates, the tag is categorized to passive or active tag. A passive tag has no power source and draws power from the reader sends electromagnetic waves, energizing the circuits in the tag. On the contrary, an active tag uses an internal power source, such as a battery, to perform all of the functions.

Also, another common RFID tag type is the semi-passive tag (or battery-assisted, as referred by Roberti M., 2011) which is similar to the passive tag in that the signal is generated passively but it differs in that it uses an internal power source to complete other functions. For all these reasons, passive tags are smaller and cheaper but their signal strength is not so strong and they cannot emit radio

waves in the range the active tags do (Wiebking L. et al., 2008). To conclude, passive tags are suitable for mass single-use applications and active tags are suitable for manufacturing (Cavoukian A., 2004).

Active tags are also categorized to beacons and transponders. On the one hand, active beacons start the communication with the reader on their own emitting radio waves and, when the reader picks up their signal, the communication starts. On the other hand, active transponders wait for the readers' signal to start the communication and they do not broadcast any signal on their own. The transponders are used to most applications but beacons are more useful for real time locating systems (OMNI-ID, 2009).

Finally, another important classification of RFID tags, according to the way they manage data, are read-only, write-once and read-write tags. A read-only tag contains pre-written data which can be read many times, a write-once tag gives the user the ability to write data only once and read them all over again many times and a read-write tag allows the user to add new data any time he wants or even write over the original data and read them over and over again many times. Typically, read-only tags are passive tags and read-write tags are active tags (Roberts C.M., 2006).

At the table below (Table 1), you can see the types of RFID tags categorized by source of power, data management and way of activation, as discussed previously. RFID tags can also come in many forms and at different shapes and sizes, depending on the reason which they are created for. Therefore, it is important to study in detail about the application to which they will be implemented before the right type of RFID system is chosen for each application.

Types of RFID tags		
Source of Power	Data Management	Way of Activation
Active tags	Read/Write	Beacons
Passive tags	Read Only	Transponders
Semi-passive	Write Once	

**Table 1** Types of RFID tags

### 3. RFID Applications

RFID technology offers powerful benefits to its adopters and today is already being used in a variety of applications. The key characteristic that differentiates one RFID application from another is the purpose of identifying the tagged items. In this chapter, a brief description of some of the most popular and common RFID applications is given.

Payment systems are one of the most popular applications of the RFID systems. Automated payment is used for highway toll collection, fare collection on public transit systems, parking in restricted areas and quick service stores. In these cases, the purpose of tagged items is to complete financial transactions in a quick and contactless way. Therefore, cars and humans are equipped with semi-passive tags that are used as credit cards and they are charged automatically.

Security and physical access control system is an application which uses RFID to identify a person who accesses a facility and even track him/her wherever he/she goes. This system is used mostly to plants and big enterprises to check on the personnel and to public locations, such as the airport, to control the crowds of people that enter etc. In this case, the purpose of identifying the tagged persons is to authenticate and spot them.

Another very popular RFID application, especially in the USA, is animal tracking. According to Lockton V. and Rosenberg R.S. (2005), pet owners implant RFID chips in their pets in order to track and locate them whenever they are lost. For the same reason, animal tracking is useful to breeders to locate missing animals. Furthermore, exotic animals and animals that are about to extinct are equipped with RFID tags to control and save their species.

There are laws of European level that make animal tracking, using RFID tags imperative and, particularly, for breeders when their goat and sheep population is more than six thousand in order to be able to check for animal epidemics. For more information, refer to the Regulation 1760/2000/EC of the European Parliament and to the Council Regulation 644/2005/EC.

At this point, it is worth noting that after animal tracking, RFID chips were implanted into humans too. The first step has already been taken and RFID chips were implanted into humans for medical reasons. For example, RFID chips were implanted into hospital patients to retrieve their medical history (Lockton V., Rosenberg R.S., 2005) and into patients with mental health problems and even into doctors and nurses to keep real-time track of their location. Likewise, trials were made to keep children safe on their way to and from school (Swedberg C., 2005b) and to track and log inmate movements during the day to prisons, as in the case of the Los Angeles County jail system that engaged in a pilot project to use RFID technology to track inmates at the Pitchess Detention Center in Castaic (Swedberg C., 2005a).

RFID chips are also already used on official documents like passports and identification documents and they store data about the person who owns it (Alexandropoulou E., Mavridis I., 2007). The International Civil Aviation Organization (ICAO) documented specifications and guidelines for machine readable travel

documents (Doc 9303, 2004, 1<sup>st</sup> Release). Then the Council of the European Union adopted a regulation on standards for security features and biometrics in passports and travel documents, issued by Member States (No 2252/2004). The so called e-passports (Juels A. et al., 2005) until now are widely used in several member states of the European Union to authenticate the identity of the holder in a contactless way.

Many manufacturers suggest that RFID creates new benefits in their factory operations too. RFID is being used in manufacturing plants to track assets and tools, increase throughput and productivity, reduce defects and manage the production line. Then, at distribution centers RFID is also useful because tags store data about the pallets that arrive and can be updated to show anytime their location, last, in retail stores RFID tags assist in shelf replenishment, in providing for the consumer's habits and also to make sure that consumers can find the right products at the right place and at the right time. All in all, RFID improves store's efficiency and is beneficial for both retailers and consumers.

Finally, supply chain management is the most common application of RFID for tracking items and automating parts, which involves all the processes a raw material has to go through to become a product and end up to the shelves of the stores and to consumers eventually. The supply chain management contains a lot of the above mentioned applications, such as manufacturing, distribution and retailing. Further detailed discussion will take place in the next chapter.

## **4. Use of RFID in the field of the Supply Chain Management**

This chapter explains the impact of RFID on the supply chain. At first, a comparison between RFID and barcoding is made because nowadays barcodes are widely used throughout the supply chain. Then, the levels of tagging are presented and, finally, the applications of RFID in the supply chain and its barriers to adoption are discussed.

### ***4.1. A comparison of Barcoding and RFID technology***

RFID is often compared to barcoding because they are both used for auto identification (Table 2). Tags in the first case and labels in the second or "Tags in the former case and labels in the latter case" contain data and they both rely on a back-end IT system that cross-references to a database (Gaukler G., Seifert R.W., 2007). Many experts argue that RFID is an extension of barcode data collection systems. However, there are significant differences between them that make them appropriate to different applications and for different reasons, with the RFID being more efficient (Holloway S., 2006).

According to Katina M. and McCathie L. (2005), the most important difference from Barcoding and, simultaneously, the most attractive advantage of the RFID technology is that it does not require line of sight to read the tags, while multiple parallel reads are possible without human involvement. For example, when a pallet arrives at a warehouse and passes through an RFID reader portal, all the products are scanned simultaneously and in milliseconds. In the case of Barcoding, on the other hand, a worker would have to open the pallet and all the boxes in the pallet and scan each item individually, because line of sight is required and the read distance must be small. This is both a laborious and a time-consuming task.

Another significant difference is the amount of data they contain. RFID tags have bigger data capacity and contain more information than barcodes do and they can even store the movement of the tagged items. Also, some RFID tags offer the capability to the user to update and add new information any time he/she wants (read/write tags). For example, whenever the tagged items move from one task to another, their tags can be updated with the time and date they started and finished each task. On the contrary, barcodes cannot be overwritten and the data they contain is set only the moment the label is printed.

Furthermore, RFID tags have sensor capabilities and, except from the movement of the tagged items, they can also record the environmental conditions that they are stored in, such as temperature and pressure. This capability is useful especially for sensitive cargo, such as food (Psion Teklogix, 2004). In addition, RFID can perform in environments where barcodes cannot. In particular, RFID can cope with harsh, dirty and oily environments but barcodes cannot be read if they are damaged, torn or dirty and they cannot be protected against the environment because they need to be exposed to achieve line of sight.

Barcode	RFID
Line of sight required	No line of sight
Individual reads	Multiple parallel reads
Update is not possible	Real-time information, read/write ability
Limited memory	Large memory
Cannot be read if damaged or dirty	Can cope with harsh environments
	Sensor capability

**Table 2** RFID Advantages versus Barcoding

However, RFID has also its own sensitivities (Hofman S.L., 2005). Liquids and metal influence its capability to read tags from a distance and problems occur when the environment is electronically noisy. So, in these cases careful study must be conducted before the positioning of the RFID readers.

To conclude, RFID and barcodes now co-exist. Barcode technology is still widely used because its implementation cost is lower, the technology is more mature and people trust it more. However, it is believed that it is only a matter of time before RFID technology spreads and takes the place of barcode technology, locally at the start and then widely. For this to happen, it is suggested that it is obligatory to create and enforce laws not only locally, but also nationally too because products containing RFID tags are exported to other countries and the consumers all over the world should be informed about it and protected.

#### ***4.2. Levels of RFID tagging***

There are three levels of RFID tagging: the pallet level, the case level and the item level. At the pallet level, the tag is attached to the pallet and can be cross-referenced to a database to retrieve information about it. The benefits of pallet level tagging are mostly the labour time that is saved because pallets are identified automatically as well as the reduction of the misplaced pallets in a warehouse optimizing the storage.

At the case level, the tag is attached to the case and, as in pallet level, it can be cross-referenced to a database to retrieve inventory information. The most important difference between pallet level and case level tagging is that at case level more detailed product traceability and inventory visibility is achieved (Gauckler G.M., Seifert R.W., 2007). Furthermore, manual checks at the retail store and labor time are saved because the need to check the number of cases on a pallet is reduced, product recalls can be managed more efficiently, and product returns are handled better since the cases being returned can be identified automatically.

At the item level tagging a tag is placed to every product either on the product itself or on its package. In this case, the benefits are even more crucial, especially, for the retailer because higher product visibility and better inventory control is achieved. In particular, readers can be placed to shelves so as to control the stock all the time and inform the personnel when a product is going to run out. Also, according to Katina M. and McCathie (2005), the personnel can be informed when products are going to expire and need to be removed immediately from these smart shelves, when the environmental conditions are inappropriate for storage and when product re-ordering is necessary. Item level tagging can be easily used as an anti-theft measure too by positioning a reader at every exit of the store.

#### ***4.3. Applications of RFID in the supply chain***

The main objective of a supply chain is to meet customer needs and as a consequence to gain more profits. Broadly speaking, supply chain's activities start with customer orders and end when the customer finally buys the product and he/she



is satisfied. With RFID, all raw materials and, finally, shipments can be identified, verified and sorted at different points in the supply chain.

A variety of stages are involved until the product reaches ends to retail stores to fill customer requests. In particular, the stages involved are product manufacturing, warehousing, distribution and retailing, and the parties concerned are manufacturers, suppliers, distributors, retailers and, finally, customers (Chalasanani S., Boppana R.V., 2007). Zebra Technologies Corporation (<http://www.zebra.com/>) is an RFID provider with more than 30 years of success in developing supply chain solutions. According to its experience, a brief description is given below of how according to its experience below is given a short description of how the RFID technology can be used to the supply chain applications and what are the benefits of its implementation (Figure 2).

At first, raw materials are equipped with RFID chips so when they arrive to the manufacturer they are checked for counterfeiting to ensure that only authorized materials enter the supply chain. After a quick check, they are directed for inventory or directly to the production line or take for back to suppliers if they are defective. If the RFID tags are read/write type, while they are driven for inventory, they are updated with location data and stored in the warehouse. In this case, RFID can provide more accurate real time information about inventory levels reducing transaction errors, processing time and labor, and minimizing the inventory inaccuracy problem (Lee Y. et al., 2004).

When raw materials are moved from the warehouse to the production line, the system is updated again in order to control stocks. In the production line encoders write data about each task, monitor the work-in-process and check the quality of the end product. Then, the finished products are stored into pallets in the warehouse and wait to be distributed to the retail stores.

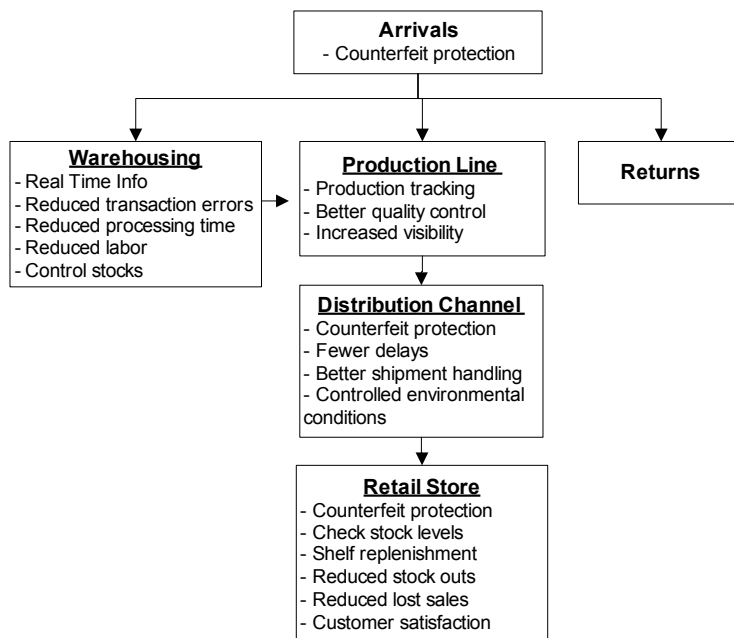
Until now two major benefits for the manufacturer are observed. The first one is the production tracking that enables products to move faster through the production line and minimizes the cost, because the check points stopping points are removed and production continuity is achieved. Another benefit, just as important, is the increased visibility through the whole supply chain. Moreover, inventory accuracy and generally data accuracy is improved and better management decisions are taken since they are based on real time information.

Once the production is completed, the finished products are packed into pallets and enter the distribution channel. The shipment is recorded again from the distributor for counterfeit and during the distribution the environmental conditions are monitored too. Many times distributors collect different shipments for different destinations and with the use of RFID the mistakes are minimized because

product identification is easier. So, the most significant benefits resulting from the application of RFID are fewer delays, better shipment handling, controlled environmental conditions and less delivery mistakes.

Finally, shipments arrive to retail stores and readers check the pallets that have just been received for counterfeit protection and the conditions which they were stored under during the distribution. The retailer in his/her turn either stores the products to his/her storeroom, or places them directly to the shelves. When a customer removes a product from a shelf (called smart shelf), the storeroom is notified so as to control the stock levels, replenish the shelves when necessary and make a new order before a product runs out (Gaukler G.M., Seifert R.W. 2007).

The benefits at this stage are also of great importance. The most remarkable benefit is the customer's satisfaction. In particular, improved in-store experience and better customer service is succeeded in several ways. Smart shelves never run out of products, the waiting time at the check out is reduced because payment is automated and after sales service is improved too since warranty data and sales information are saved, as Tajina M. also suggests (2007), reduced stock outs and subsequently reduced lost sales allow retailers to pay more attention and invest to other problems, such as store management and new product introduction.



**Figure 2** Advantages of the implementation of the RFID at each stage of the supply chain

To summarize, with the use of RFID in the supply chain, all applications are automated, product flow is uninterrupted and customers find the right products at the right place, at the right time and in the most cost effective manner. So, shop experience is improved, customer needs are satisfied, competitive advantage is gained, profits are increased and, consequently, everyone benefits.

#### ***4.4. Barriers to RFID adoption in the supply chain***

There are many challenges and barriers that keep down the evolution of RFID in the supply chain. Huber N. et al. (2007), after a research conducted in industries found that these barriers to adoption are mainly the cost, the lack of awareness and consumer privacy concerns.

The cost of various RFID components is one of the most significant barriers for its adoption. RFID tags in a supply chain, even when used at the pallet level or at the item level, are the most costly components because they need to be replaced constantly. Also, RFID readers and the backend IT system cost too, but only at the installation phase and when they require maintenance. Further, it is estimated. Nonetheless, it is estimated that when RFID tags are implemented and produced on a larger scale, their production cost is diminished and their cost isat considerable.

Simultaneously, there are considerable gaps in the awareness of the RFID technology. This lack of awareness requires information sources to be directed at manufacturers and retailers too (Huber N. et al., 2007). Therefore, it is believed that knowledge about the implementation of the technology, its benefits in the retail supply chain environment and its vulnerabilities should be provided by consultants. An effective awareness effort can ensure successful integration of the technology in the supply chain eventually.

Finally, a major barrier for RFID adoption in the supply chain is the consumer privacy concerns that arise as well as the lack of any legal regulations. With the implementation of the RFID in the supply chain, data protection and privacy became one of the major challenges and many concerns about the security and privacy of personal information arose. More details about the technology's effect on privacy and the legal efforts adopted will be discussed in the next chapter.

### **5. Privacy Risks and Legal Concerns over RFID data collection**

As inferred, RFID technology not only has benefits but raises also serious legal concerns, especially for its consumers. The fact that the content of RFID tags can be accessible by third parties without the consent of the person who carries it, raises serious legal privacy concerns/issues. The aim of this chapter is to present

the most significant privacy risks and legal concerns that evolve with the use of the RFID technology.

According to Kelly E. and Erickson S. (2005), RFID technology threatens consumers through intrusion in their informational privacy space. Informational privacy (or data privacy) is the consumer's right to retain control over his/her personal information. Further, the consumer's right to privacy includes the right to know exactly which of his/her personal information is collected and be informed about the identity of the data controller that is, (the person who collects and is responsible to keep safe his/her personal information). The consumer can even demand the removal of the data from the database if they are unverifiable, or the person who collects the correction if they are inaccurate.

Passive tags can be read from 10 meters distance and this way can be limited to 10cm for security, but active tags can be read from 100 meters. Moreover, active tags are used when it is necessary to know anytime the location of the object tagged (Lockton V., Rosenberg R.S., 2005). For example, at the distribution channel, it is important for the distributor to know and locate where the shipments are to succeed better shipment handling. In this case, the privacy risk is the possibility of eavesdropping from competitors.

When RFID tags are used in pallets during manufacturing, warehousing and distribution, not so major privacy issues arise. If the tagging is limited to the pallet level, then only a few privacy concerns arise because it is unlikely for the RFID tag to come to the possession of the consumer. The problem starts with item-level tagging where all products are tagged and will still have the tag on them when the consumer purchases them and leaves the store (Kamaledevi B., 2010). Thus, when products with RFID tags are used to retail stores, as barcodes do now, and pass on to the hands of the consumer, great privacy concerns arise and it is vital to enforce legal restrictions to protect consumers.

Additionally, RFID technology threatens consumers through intrusion in their civil liberties (Kelly E., Erickson S., 2005). In particular, a major privacy concern is the secret surveillance of the consumer that possesses items with RFID tags. If the RFID tag continues to be attached to the products after the purchase, it makes it possible for the retailers to monitor their customers. For example, think of a store that uses item level tagging and has readers at all its exits to prevent theft. If a consumer buys a watch from that store, whenever he/she enters the store wearing that watch, the reader will communicate with its RFID tag and will know when that person visits the store and will even be able to record the products that he/she purchases every time. In this way, the retailer will be able to record the consumer's habits and activities and create his/her consumer profile. Furthermore, if the store connects its payment system with the RFID information, then

the identity of the RFID holder will no longer be unknown and if the retailers start sharing this information, then, that person will be exposed.

Consumer tracing and tracking should be avoided taking all, the necessary measures no matter what the cost is. Many people believe that only the technological means can protect consumers from privacy threats. However, through the evolution of the information technologies it is proven that technical mechanisms will always be vulnerable to attacks. On the one hand technical measures are essential but, on the other hand, they are not enough to safeguard privacy. A legal framework is necessary too and should be taken into consideration even at the design phase of the technology. But as Lockton V. and Rosenberg R.S. suggest, even after the adoption of a legal framework, it is likely that the manufacturer and the retailer will take full advantage of all the benefits the technology provides, whether legal or not, with a goal of gaining competitive advantage in the market.

The consumer is vulnerable to theft too. In particular, if thieves are equipped with readers, they will be able to read the contents of the shopping bag or the value of the watch that his/her possible victim wears. Burglars can benefit too by choosing the house which they are going to break in, based on the content of the home via an RFID reader. In this case, RFID technology threatens consumers through intrusion in their physical privacy (Kelly E., Erickson S., 2005) and the problem will get even bigger if RFID tags are attached to money too.

## **6. Legal efforts in the USA, in Japan and in EU**

This chapter focuses on the legal efforts that are made in the USA, in Japan and in EU. At first, the most relevant proposed legislation by several US states is presented and then Japan's guidelines for the protection of privacy and EU's principles, as are discussed summarized from working documents and relevant recommendations.

### **6.1. USA**

The first reaction for the implementation of the RFID technology appeared in the USA. There they lack in data protection and therefore American consumers reacted when the RFID technology entered in their personal lives. Efforts have been made in several States, such as California, Georgia, New Jersey, Washington and New York, to create privacy legislation or make relevant proposals for the right use of the RFID technology.

The first proposed legislation concerning RFID was introduced by California's state senate Debra Bowen. The law required business entities that use the technology to inform the consumer about its use, obtain his written consent before the collection and process of his personal data and give him the option to destroy

or detach the tag before he/she leaves the store. The last two requirements, the obligation to obtain written consent and the option to detach or destroy the tags, were deleted from a new version of the bill that passed senate.

In 2010, at least 11 states introduced legislation related to RFID. Some of the most relevant in our case are, in Georgia the House Bill (HB) 16 that prohibits the electronic tracking and monitoring of another person without the consent of the related person, in New Jersey the Assembly Bill (AB) 1732 that requires businesses to notify customers when RFID technology is used and collects information about them, in New York the AB 274 that requires the labeling of retail products or packages that contain RFID tags and the SB 8196 that enacts the RFID Right To Know Act, requiring to disclose the use for RFID devices, label all the retail products that contain RFID tags, set standards for labels, set points of sale removal of RFID tags and restrict aggregation and disclosure of personal information.

Finally, in Washington State, Representative Jeff Morris introduced the House Bills 1006 and 1011. The aim of these bills is to inform consumers that the RFID technology is in use and that they can decide whether they want to possess a product with an RFID tag or not. In particular, HB 1006 requires that a government or business entity that sells RFID-tagged products must label them, unless the tags are disabled, deactivated, or removed at the point of sale. The label must be universally recognizable by the public and clearly indicate that the RFID technology is used and those products are tagged.

The second bill HB 1011, introduced in 2009, prohibits governmental or business entities from reading an RFID tag that is possessed by a consumer, without first obtaining his opt-in consent. The opt-in consent must be either in writing or electronically and the government or the business entity must disclose that by consenting that he agrees to let the governmental or business entity collect, use, or retain data gathered for any purpose. Also, the bill requires that opt-in consent is not required in cases, he/she such as health or safety reasons, triage or medical care during a disaster, incarceration and court order. For more information about privacy legislation related to RFID from 2004 until now, one may visit National Conference of State Legislatures (<http://www.ncsl.org/default.aspx?tabid=21255>).

To conclude, American consumers created a group in 1999 called Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN). Now, this group focuses on the use of the RFID chips from the supermarkets and its aim is to educate consumers about the vulnerabilities and the privacy risks that arise from its use and encourage privacy-conscious shopping habits (<http://www.nocards.org/>). CASPIAN proposed the RFID Right to Know Act of 2003 according to which business entities should use labels on products that contain RFID tags to

state that the tag can transmit information to a reader both before and after purchase. They also suggested that those labels should be in a conspicuous type-size and prominent location and in print that contrasts with the background against which it appears.

## **6.2. Japan**

In 2004, in Japan, the Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPT) and the Ministry of Economy, Trade and Industry (METI) issued the "Guidelines for the Protection of Privacy with Regard to RFID Tags". The objectives of the guidelines are to protect consumer privacy while encouraging the use of RFID tags. According to these guidelines and as Natsui T. (2006) explains, the consumer must be informed about the presence of RFID tags, their location, their nature and the information that they record. The consumer also has the right to choose if he/she wants to make the tag unreadable after he/she purchases the product and the business entity has the right to try to persuade him/her not to destroy the tag, by explaining to him/her what the benefits of its use are. Furthermore, business entities that use RFID tags must inform consumers about their uses, their benefits and their disadvantages, so as to maximize consumer awareness and facilitate technology's sound development.

## **6.3. European Union**

As Murakami Y. (2004) states, unlike Japanese people, Europeans are highly aware of/about privacy issues. The European Union is studying privacy and data protection principles related to RFID technology. In January 2005, the EU's Article 29 Data Protection Working Party published a Working Document (WP 105) on data protection issues related to RFID technology where the advantages offered by the RFID technology and the privacy concerns are presented. Further, the importance of the implementation of the basic principles set out in the EU Data Protection Directive and the Directive on privacy and electronic communications are highlighted and the technical characteristics of the technology, its multiple uses in many sectors and the privacy implications are presented. Finally, guidelines for legal processing and data security are suggested.

In 2006, Viviane Reding, the European Commissioner for Information Society and Media, launched a public debate on RFID, and in 2007, a communication from the Council commission to the European parliament, the commission council, the European economic and social committee and the committee of the region summarized the importance of a European RFID policy and its further development.

Later, on May 12<sup>th</sup> 2009, the European Commission issued a recommendation on the implementation of privacy and data protection principles in applications supported by RFID. This recommendation invited Member States to ensure that the industry develops a framework for privacy and data protection impact assessment and provides guidance on the design and operation of RFID applications in a lawful, ethical furthermore, and, socially and politically accepted way, and in a guidance about data protection impact assessments, information security, transparency on RFID use and awareness raising actions are also suggested.

In particular, the Commission recommends the Member States to ensure that RFID operators conduct privacy and data protection impact assessment before an RFID application is deployed, assign a person to review it and make its results available to the competent authority. They should also ensure that they take measures to raise awareness, provide examples of good practise, ensure the development of an easy to understand information policy, determine whether RFID tags placed on products represent a likely threat to privacy. If so, deactivation and removal at the point of sale should be done immediately without any charge.

On March 31<sup>st</sup> 2010, a privacy and data Protection Impact Assessment (PIA) Framework for RFID applications was proposed by an informal RFID work group led by industry representatives, based on the Commission's Recommendation. According to them, the proposed PIA Framework would help the adopters of the RFID technology to establish and maintain compliance with privacy and data protection laws and to provide its benefits, while integrating privacy by design at the early stages of the development.

On July 13<sup>th</sup> 2010, the EU's Article 29 Data Protection Working Party published an opinion in response to the proposed PIA Framework (Opinion 5/2010, WP 175). The Working Party concluded that the proposed PIA Framework was not fully accepted in its current form and that it should be improved. Specifically, it states that the proposed PIA Framework doesn't make it clear to the RFID adopters how to assess privacy issues and establish compliance with data protection laws and it doesn't explicitly address the tag deactivation principles. Also, it recommends that the PIA Framework should that it does not give guidance to the adopters to decide when is the most appropriate time and conditions to conduct a PIA. So, the Working Party concluded that the industry should propose an improved PIA Framework, taking into account all of its comments.

Later the same month, the European Network and Information Security Agency (ENISA) published an opinion with practical recommendations to improve the proposed PIA Framework. As a consequence, on January 12<sup>th</sup> 2011, the industry proposed a revised PIA Framework, taking into account all of the recommendations and comments provided both by the Working Party and ENISA.



The revised PIA Framework addresses the process for conducting PIAs for RFID applications before deployment and separately for each RFID application they operate, and specifies the scope of resulting PIA Reports, as the European Commission recommended. In addition, because many RFID application operators within particular sectors may be considering similar applications, this framework provides a basis for the development of PIA Templates so as to produce PIA Reports more efficiently.

On February 11<sup>th</sup> 2011, the EU's Article 29 Data Protection Working Party published an opinion in response to the revised PIA Framework (Opinion 9/2011, WP 180). This time the Working Party suggests that the revised Framework not only addresses the most concerns, but that it also presents stronger guidelines for the RFID operators who will implement this PIA Framework. Also, the Framework clearly claims RFID operators to evaluate the risks that may arise when the tags may be used (or misused) by third parties and especially in the retail sector when they are carried by consumers. Thus, the Working Party accepted and endorsed this revised PIA Framework and suggested to translate the PIA reports in other languages too, since some RFID Applications will be implemented in several Member States.

## **7. Conclusions and legal proposals**

Taking it all into consideration, it is concluded that a legal framework is vital to limit the way the RFID technology is used by government and business entities. With the implementation of the RFID in the supply chain, data protection and privacy became two of the major challenges to meet. The technological means are necessary and should be implemented in respect of privacy and regulation, but cannot protect the consumers enough. Serious privacy risks are posed when the technology is used and legal regulation should be considered even at the design phase of the technology.

In EU several attempts have been made to create guidelines and data protection principles related to the implementation of the RFID technology so as to be generally accepted and adopted by all Member States. The first attempt was made in 2005 when the EU's Article 29 Data Protection Working Party published a Working Document on data protection issues related to RFID technology. And the last attempt until today was on January 12<sup>th</sup> 2011, when a privacy and data Protection Impact Assessment Framework for RFID applications was proposed and the Working Party endorsed it a month later.

At the same time, it is observed that the most common policies accepted by many US states are the prohibition of the tracking and monitoring of another person without his/her consent and the labeling of retail products that contain RFID

tags. Notification which clearly indicates that the RFID technology is used and collects information and that the particular products are tagged is required and the choice to remove the RFID tag after the purchase of a tagged product is given.

Because each US state, and, generally, each country, has its own legislation and principles or no legislation at all, problems can be caused with imports and exports. It is suggested that laws should be created and enforced nationally so as to protect consumers/their citizens when products containing RFID tags are exported to other states or countries.

Also, it is recommended to apply the Personal Data Protection Law whenever the RFID technology is implemented to an application anywhere in the world. The basic principles that settle the collection and use of personal information and assure adequate privacy protection should be implemented and adjusted to the technology's special features (Alexandropoulou E., Mavridis I., 2007). In particular, the purpose of the collection must be disclosed and data should be used only for the purpose stated. In the case the business entity wants to use them for other purposes, it must first obtain the data subject's consent. Furthermore, the business entity who stores and processes personal information is responsible to keep them accurate and up to date, inform a person about the information collected that concerns him/her and save it in a safe place.

To sum up, with the evolution of the RFID technology and its intrusion to our personal lives, a new era began when technology outstripped the existing law. The existing law does not protect the consumer enough and changes or additions should be made. Further, it is important that new principles and bills are carefully set and established so as to facilitate the development of this promising technology and protect consumer's privacy.

## References

### *A. Books and Papers*

Alexandropoulou-Egyptiadou, E. (2007), *Personal Data (Regulatory framework of their e-processing)*, A.N. Sakkoula, Athens-Komotini

Alexandropoulou-Egyptiadou, E., Mavridis I. (2007) "Data protection from the implementation of the RFID technology. Legal and Technological Approach", *Armenopoulos*, 493-504

Bottis M., Nota scalpe L.: *RFID technology and patient care*, TEKMRHION 2010 Cunder Publication).

Cavoukian, A. (2004) "Tag, You're It: Privacy implications on Radio Frequency Identification (RFID) Technology", *Information and Privacy Commissioner/ Ontario*

Chalasani, S., Boppana, R.V. (2007) "Data Architectures for RFID Transactions", *IEEE Transactions on Industrial Informatics*, 3 (3), 246-257

Gaukler, G., Seifert, R.W. (2007), Applications of RFID in supply chains in *Trends in supply chain Design and Management: Technologies and Methodologies*, Chapter 2, Edited by Hosang Jung, Frank Chen, Bongju Jeong, Springer London Ltd., online at <http://ise.tamu.edu/people/faculty/gaukler/Applications%20of%20RFID%20in%20Supply%20Chains%20-%20Gaukler%20and%20Seifert.pdf>, last access 24.03.2011

Eileen, P.K., Erickson, S. (2005) "RFID tags: commercial applications v. privacy rights", *Industrial Management and Data Systems*, 105 (6), 703-713

Hofman, S.L. (2005) "iSeries RFID- Status Report", *iSeries News Magazine*, 1-3, online at [http://www.tlashford.com/Web\\_new\\_ideas/download\\_free/TLA\\_iSeries\\_RFID\\_Status\\_Report.pdf](http://www.tlashford.com/Web_new_ideas/download_free/TLA_iSeries_RFID_Status_Report.pdf), last access 24.03.2011

Holloway, S. (2006) "RFID: An Introduction", online at <http://msdn.microsoft.com/en-us/library/aa479355.aspx>, last access 24.03.2011

Huber, N., Michael, K., McCathie, L. (2007) "Barriers to RFID Adoption in the Supply Chain", *IEEE RFID Eurasia*, Istanbul, Turkey, 1-6

Juels, A., Molnar, D., Wagner, D. (2005) "Security and Privacy issues in E-Passports", In proceedings of IEEE SECURECOMM 2005, First International Conference on Security and Privacy for Emerging Areas in Communications Networks, Athens, Greece, 74-88

Juels, A. (2006) "R.F.I.D. Security and Privacy: A Research Survey", *IEEE Journal on Selected Areas in Communications*, 24 (2), 381-394

Kamaladevi, B. (2010) "RFID-The best technology in supply chain management", *International Journal of Innovation, Management and Technology*, 1 (2), 198-204

Katina, M., McCathie, L. (2005) "The pros and cons of RFID in Supply Chain Management", *International Conference on Mobile Business*, 623-629

Kelly, E.P., Erickson, G.S. (2005) "RFID tags: commercial application v. privacy rights", *Industrial Management & Data Systems*, 105 (6), 703-713

Lee, Y., Cheng, F., Leung, Y. (2004) "Exploring the impact of RFID on supply chain dynamics", *Proceedings of the 2004 Winter Simulation Conference*, 2, 1145-1152

LEGAL-IST project, Report on Legal Issues of RFID Technology, Doc. No D15, May 2006, pp. 11, online at [http://www.rfid-in-action.eu/public/rfid-knowledge-platform/all-rfid-documents/generic-information-on-rfid-systems/LEGAL-IST\\_Legal%20issues%20of%20RFID%20technology.pdf](http://www.rfid-in-action.eu/public/rfid-knowledge-platform/all-rfid-documents/generic-information-on-rfid-systems/LEGAL-IST_Legal%20issues%20of%20RFID%20technology.pdf), last access 24.03.2011

Lockton, V., Rosenberg, R.S. (2005) "RFID: The next serious threat to privacy", *Ethics and Information Technology*, 7, 221-23

Michael, K., McCathie, L. (2005) "The pros and cons of RFID in supply chain management", *Proceedings of the International Conference on Mobile Business (IC-MB'05)*, IEEE Computer Society, online at <http://ro.uow.edu.au/infopapers/105>

Murakami, Y. (2004) "Privacy issues in the ubiquitous information society and law in Japan", *Proceedings of the IEEE International Conference on Systems, Man & Cybernetics: The Hague, Netherlands*, 5645-5650

Natsui, T. (2006) "RFID Tags: Legal issues and Guidelines in Japan", *Meiji Law Journal*, 13, 31-5

OMNI-ID White paper (2009) "The Technology of On-Metal RFID", online at [http://www.omni-id.com/pdfs/RFID\\_Tag\\_On-Metal\\_Technology\\_WhitePaper.pdf](http://www.omni-id.com/pdfs/RFID_Tag_On-Metal_Technology_WhitePaper.pdf)

Psion Teklogix (2004) "Understanding RFID and Associated Applications", online at [http://barcodingworks.com/?module=file&act=procFileDownload&file\\_srl=834&sid=f4c018c2525553c93e3b669d3ddd518d](http://barcodingworks.com/?module=file&act=procFileDownload&file_srl=834&sid=f4c018c2525553c93e3b669d3ddd518d), last access 24.03.2011

Rieback, M.R., Crispo, B., Tanenbaum, A.S. (2005) "Uniting Legislation with RFID Privacy-Enhancing Technologies", *Proc. 3rd Conference on Security and Protection of Information. (SPI 2005)*, Brno, Czech Republic

Roberti, M. (2011) "What Is a Semi-passive RFID Tag?", *RFID Journal*, online at <http://www.rfidjournal.com/expert/entry/8117/>

Roberts, C.M. (2006) "Radio Frequency Identification (RFID)", *Computers and Security*, 25, 8-26

RSA Laboratories, Research Areas: RFID Privacy and Security, online at <http://www.rsa.com/rsalabs/node.asp?id=2115>, last access 24.03.2011

Swedberg, C. (2005a) "L.A. County Jail to Track Inmates", *RFID Journal*, online at <http://www.rfidjournal.com/article/view/1601>, last access 24.03.2011

Swedberg, C. (2005b) "RFID Watches over School Kids in Japan", *RFID Journal*, online at <http://www.rfidjournal.com/article/articleprint/2050/-1/1/>, last access 24.03.2011

Tajima, M. (2007) "Strategic value of RFID in Supply Chain Management", *Journal of Purchasing & Supply Chain Management*, 13, 261-273

Wiebking, L., Metz, G., Korpela, M., Nikkanen, M., Penttilä, K. (2008) "A Roadmap for RFID Applications and Technologies", *CE RFID Final Report, Work Package 1*, 53-57

Zebra Technologies Corporation (2007) "Enhancing the retail supply chain", online at [http://www.zebra.com/id/zebra/na/en/documentlibrary/product\\_brochures/rfid\\_supply\\_chain.File.tmp/RFIDsupplyChainR2\\_2%2015\\_FINAL.pdf](http://www.zebra.com/id/zebra/na/en/documentlibrary/product_brochures/rfid_supply_chain.File.tmp/RFIDsupplyChainR2_2%2015_FINAL.pdf), last access 24.03.2011

## ***B. Legal Texts and Decisions***

Commission Recommendation on the implementation of privacy and data protection principles in applications supported by RFID, Commission of the European Communities, 12 May 2009, C (2009) 3200, online at: [http://ec.europa.eu/information\\_society/policy/rfid/documents/recommendationonrfid2009.pdf](http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf), last access 24.03.2011

Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions "Radio Frequency Identification (RFID) in Europe: steps towards a policy framework", COM(2007) 96 final, online at [http://ec.europa.eu/information\\_society/policy/rfid/documents/infso\\_com\\_2007\\_96.pdf](http://ec.europa.eu/information_society/policy/rfid/documents/infso_com_2007_96.pdf), last access 24.03.2011

Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, online at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:EN:PDF> last access 24.03.2011

Council Regulation 644/2005/EC of 27 April 2005 authorizing a special identification system for bovine animals kept for cultural and historical purposes on approved premises as provided for in Regulation 1760/2000/EC of the European Parliament and the Council, OJ 107

ENISA Opinion on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications of March 31, 2010, July 2010, online at <http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia>, last access 24.03.2011

Georgia HB 16, online at [http://www1.legis.ga.gov/legis/2009\\_10/fulltext/hb16.htm](http://www1.legis.ga.gov/legis/2009_10/fulltext/hb16.htm), last access 24.03.2011

Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications (2010), online at [http://ec.europa.eu/information\\_society/policy/rfid/documents/d31031industrypia.pdf](http://ec.europa.eu/information_society/policy/rfid/documents/d31031industrypia.pdf), last access 24.03.2011

Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications (2011), online at <http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf>, last access 24.03.2011

International Civil Aviation Organization (ICAO), Machine readable travel documents, Doc 9303 (2004), 1st Release, online at <http://www2.icao.int/en/MRTD/Downloads/Forms/AllItems.aspx?RootFolder=http%3a%2f%2fwww2.icao.int%2fen%2fMRTD%2fDownloads%2fDoc%209303&FolderCTID=0x0120000764101A62EA554BB5D36C62DB0F9735> (there have been 8 releases of the document from 2004 until 2010), last access 24.03.2011

Japan (2004), Guidelines for Privacy Protection with Regard to RFID Tags, online at: [http://www.rfid-in-action.eu/internal/documents/activities-2/rfid-guidelines/all-rfid-documents/guidelines-on-privacy/Government%20of%20Japan\\_Guidelines%20for%20Privacy%20Protection%20with%20Regard%20to%20RFID%20Tags.pdf](http://www.rfid-in-action.eu/internal/documents/activities-2/rfid-guidelines/all-rfid-documents/guidelines-on-privacy/Government%20of%20Japan_Guidelines%20for%20Privacy%20Protection%20with%20Regard%20to%20RFID%20Tags.pdf), last access 24.03.2011

National Conference of State Legislatures, online at <http://www.ncsl.org/default.aspx?tabid=13442>, last access 24.03.2011

New Jersey AB 1732, online at <http://www.njleg.state.nj.us/bills/BillView.asp> accessed 24.03.2011, last access 24.03.2011

New York AB 274, online at <http://e-lobbyist.com/gaits/text/33652>, last access 24.03.2011

New York SB 8196, online at [http://assembly.state.ny.us/leg/?default\\_fld=&bn=A01033&Summary=Y&Text=Y](http://assembly.state.ny.us/leg/?default_fld=&bn=A01033&Summary=Y&Text=Y) last access 24.03.2011

Opinion on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, ARTICLE 29 Data Protection Working Party, WP 112, Official Journal L 385, 29/12/2004, 1–6, online at [http://www.bite-project.org/next\\_events/WORKING%20PARTY%2029%20wp112\\_en.pdf](http://www.bite-project.org/next_events/WORKING%20PARTY%2029%20wp112_en.pdf), last access 24.03.2011

Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, July 13 2010, ARTICLE 29 Data Protection Working Party, 00066/10/EN, WP 175, online at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_en.pdf), last access 24.03.2011

Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, ARTICLE 29 Data Protection Working Party, 00327/11/EN, WP 180, online at: [http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-a29wp-opinion-11-02-2011\\_en.pdf](http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-a29wp-opinion-11-02-2011_en.pdf), last access 24.03.2011

Regulation 1760/2000/EC of the European Parliament and the Council establishing a system for the identification and registration of bovine animals and regarding the labelling of beef and beef products and repealing Council Regulation 820/97/EC, online at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2000R1760:20070101:EN:PDF>, last access 24.03.2011

Washington State HB 1006, online at <http://apps.leg.wa.gov/documents/billdocs/2009-10/Pdf/Bills/House/Bills/1006.pdf>, last access 24.03.2011

Washington State HB 1011, online at <http://apps.leg.wa.gov/documents/billdocs/2009-10/Pdf/Bills/House%20Bills/1011.pdf>, last access 24.03.2011

Working document on data protection issues related to RFID technology, 19 January 2005, ARTICLE 29 Data Protection Working Party, 10107/05/EN, WP 105, online at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf) accessed 24.03.2011, last access 24.03.2011

# **Ethics in scholarly publishing: the journal editor' s role**

---

---

**Anna-Maria Olenoglou**

---

---

## **1. Introduction**

The significant increase in published information, both in digital and printed form, entails many risks and challenges that publishing houses should identify and deal with, in order to preserve their scholarly integrity and gain the trust and satisfaction of their reading audience. The publishing industry is extremely important for the diffusion of research and knowledge. Through their publications, scientists disseminate their work and are being evaluated by the scientific community and the general public [1]. Publishing enables the circulation of ideas, promotes scientific dialogue and supports educational practices.

During the past two decades there has been a significant increase in the number of peer-reviewed and open access scholarly journals, newsletters and internet resources in almost every scientific field. A publishing house may comprise hundreds of journal titles diffused mainly electronically. Especially in rapidly growing fields, such as informatics and ICTs, scholarly journals are considered to be an ideal way to publish papers and studies as compared to books [2]. The rapid increase in scholarly publications and their direct dissemination with the use of new technologies has many advantages but also put forward the issue of publication quality. Competitiveness, research underfunding and the need to create a reputation and evolve professionally urge scholars to constantly pursue publication in scholarly journals, opting for quantity instead of quality in some cases [1], disregarding the ethics of scholarly writing and publishing as a result.

This paper focuses on the journal editors who are expected to deal with this issue and make crucial decisions on publications and journal contents. Among other responsibilities they are expected to evaluate the quality of the material submitted for publication and therefore investigate the author's ethics in order to ensure the quality and accuracy of the publication [3].

## **2. Ethics in scholarly publishing: scientific misconduct**

Ethics, as a philosophy branch, is dealing with a series of issues that have been of concern to humankind since the antiquity. Publishing ethics seem to have several philosophical and practical implications as well, depending on the field of each



scholarly journal. For instance, medical journals face different issues as compared to technology journals or history journals etc. This bibliographical research will be focusing on an ethics issue that concerns scholarly publishing as a whole regardless of the different scientific fields: the issue of scientific misconduct.

“Misconduct in science” or “scientific misconduct” (the older term “scientific fraud” is no longer in use due to a shift in the meaning of the word “fraud”) is a technical, semi-legal term designating behaviours that justify federal intervention, and its precise definition is a matter of crucial importance [4]. Misconduct in scientific research is actually a deliberate significant misbehaviour on the part of the scientist that impedes research progress or falsifies scientific data and compromises the integrity of science. More specifically:

“Misconduct in science means fabrication, falsification, plagiarism, or other practices that seriously deviate from those that are commonly accepted within the scientific community for proposing, conducting or reporting research. It does not include honest error or honest differences in interpretation” [5].

Although scientific misconduct has different meanings in different countries, in the definition provided above one can discern some fundamental aspects of the term, such as *fabrication*, i.e. the presentation and publication of a research or an experiment that have never been conducted or *falsification*, used to designate a deliberate data distortion or an omission of information and finally *plagiarism*, used to describe the appropriation and presentation of the ideas of others without mentioning their names. The practice of *self-plagiarism* is also very common and occurs when authors reuse in their recent work data that have already been presented in their pervious publications [6].

Nevertheless, these are not the only types of unethical behaviour that authors tend to adopt according to the literature [7]. *Duplicate publication* (also known as redundant publication) is also a common type of scientific misconduct that consists in over-publishing the same work or a slightly revised version of it in more than one journal, book or webpage. This behaviour is unethical in the sense that the author constantly reproduces the same content without providing the readers with any new knowledge. Publishing houses have adopted the common policy of the single submission, which actually means that a manuscript should be submitted to one journal at a time so as to avoid parallel publication. After the author receives a written rejection he can resubmit the manuscript to another journal. The lingering unanswered question is how many publications can be related to only one research project [6].

Another form of unethical behaviour is related to the authorship issues that mainly arise when a manuscript has multiple authors. According to the International Society of Addiction Journal Editors, "The authorship of a scientific report refers to the origin of a literary production, not just to the experimentation, data collection or other work that led up to it. All persons named as authors should 1) have made a major contribution to the work reported, and 2) be prepared to take public responsibility for its contents" [7]. However, in many cases it is rather difficult to define the exact extent of a "major contribution" especially when the publication is part of a larger group project. The practices of *ghost authorship*, that is, omitting the name of an author who has participated in the research and *guest authorship*, i.e. adding author names that did not contribute to the research mainly because of their reputation, are quite common [8].

Throughout the literature, scientific misconduct is also believed to stem from a potential conflict of interest, either intellectual or financial. An intellectual conflict of interest occurs in cases where the content of a manuscript contradicts general knowledge. Authors site their sources in order to support their work. However, some of their references might be inaccurate or unable to support their hypotheses. A financial conflict of interest occurs when the author receives funding from a corporate sponsor (e.g. a pharmaceutical company) [7]. In this case it is considered unethical to promote a specific product or present only the positive results of the research to the corporate sponsor [6].

Furthermore, a research might be suspected for misconduct when it is extremely good and when its methodology is not presented or there are problems in its methodology (e.g. insufficient sample size) or data analysis. Even though the majority of such manuscripts are being rejected [9] in some cases the solution to the problem is not that simple and the editor is called to actually deal with scientific misconduct.

### 3. The editor's role

Publishing is a rather complicated procedure due to the number of different professionals that take part in it [10]. The role of the editor is extremely important in this process, since it is directly related to the quality of the publication especially in scholarly publishing [11, 12]. What is more, editors are required to work with authors, reviewers and the publisher, coordinate and maintain the balance among all the professionals that participate in the process [13]. Journal editors have increased responsibilities as they are responsible for the journal's content so as to preserve the reputation and status of the publishing house and satisfy the requirements of the reading audience. At the same time, editors are expected to

deal with unethical behaviour on the part of researchers and scientists and want assurance that the information and knowledge provided are accurate and trustworthy [6].

It was only during the 1980s when the issue of unethical practices in journal publishing came to the fore especially in the field of medical publishing and discussions on the creation of a code of ethics that would determine the obligations of the authors towards their readers and other authors became more frequent [14]. During the same decade the issue of the ethical responsibilities of editors and the creation of explicit guidelines for authors, editors, and reviewers started to gain importance [15]. After all, scholarly journals have increased responsibilities towards their field and their reading audience and should develop writing and editing policies. In 1978 a group of medical journal editors met informally in Vancouver, British Columbia, in order to establish guidelines on the format of the manuscripts submitted to their journals. This group became known as the Vancouver Group. It expanded and evolved into the International Committee of Medical Journal Editors (ICMJE), an organisation that still provides guidelines to medical journal editors [16]. Since that time, several international associations and organisations were established and attempted to determine the responsibilities and competencies of the editors in order to help them deal with unethical behaviour. Some of these associations are mentioned in the following paragraphs.

The World Association of Medical Editors (WAME) established in 1995, is a non-profit voluntary association of peer-reviewed medical journal editors from countries throughout the world who seek to foster international cooperation and promote the education and training of medical journal editors. The WAME has 1664 members representing more than 980 journals from 92 countries [17].

The International Society of Addiction Journal Editors (ISAJE) is the first society for addiction journal editors and was formally constituted in 2001 as a non-profit organization. The ISAJE holds major meetings every year providing an opportunity to discuss and share problems. The Society addresses the needs of journal editors, their staff, authors and reviewers and provides support and guidance. It also organises training seminars and offers guidance on ethical regulations and publication standards through online and printed material. The association especially supports journals published in the developing world and in languages other than English [18].

The Council of Biology Editors (CBE) was renamed into the Council of Science Editors in 2000 due to the integration of members from other scientific fields and has more than 1,200 members. The CSE's main mission is to serve editorial professionals in the sciences by creating a supportive network for career develop-

ment, providing educational opportunities and developing resources for identifying and implementing high-quality editorial practices [19].

The Committee on Publication Ethics (COPE) was established in 1997 by a group of medical journal editors in the UK but it now has over 6,000 members worldwide from all academic fields. Membership is open to academic journal editors and every one else interested in publication ethics. Several major publishers have signed up their journals as COPE members [20].

All editor associations agree on the role and the responsibilities of journal editors. Journal publishers and editors are equally responsible for the publication of an accurate and trustworthy journal but hold different roles. Publishers have the right to hire and dismiss editors and make important commercial decisions that require an active participation on the part of the editor. The ICMJE notes that editors should have full responsibility in determining the editorial content of a journal. The notion of editorial freedom should be resolutely defended by editors, even when putting their positions at stake.

The initial role of editors is to check whether a submitted manuscript is appropriate for the journal, that is, whether it falls within the journal's scope of interest. The decision to publish a manuscript is closely related to some of its characteristics (importance of the topic, originality, scientific strength, clarity and completeness of written expression). Then, editors choose some expert reviewers (i.e. referees) who will evaluate the submitted manuscript and are in direct communication with the author and the review team in order to achieve an effective and smooth cooperation [16]. Editors are the first people to see the manuscripts and conduct an initial screening in order to decide on their course.

The WAME urges editors to consider whether certain researches are ethical and whether their publication could harm the readers or the public interest. Furthermore, it states that editorial decisions should not be influenced by the nationality, ethnicity, political beliefs, race or religion of the author. Editors should also encourage reviewers to conduct detailed screenings on the manuscript's originality and any type of potential scientific misconduct [21]. Finally they should check the efficiency and quality of the reviewers and examine cases of suspected reviewer misconduct.

The responsibilities of editors, as presented by the WAME, demand that they should respect readers, authors and reviewers and disclose all journal procedures (e.g., governance, editorial staff members, number of reviewers, review times, acceptance rate). They should also promote self-correction in science and attempt to improve scientific research practices through the publication of their corrections, retractions and reviews of published papers. Editors should confirm

the honesty and integrity of the journal content and minimize any type of bias through managing conflict of interests and maintaining information confidentiality. Finally, they are required to improve the journal's quality through their involvement in editing, peer review, research ethics, methods of investigation and the rationale and evidence base that supports them, establishing the adequate efficiency evaluation projects and pursuing external efficiency evaluations [3].

#### **4. Dealing with scientific misconduct**

Over the past decade, a number of peer reviewed academic journals have adopted a common policy on ethics. The webpages of several publishing houses contain writing guidelines for authors and define the responsibilities and competencies of editors and reviewers. In late 2006 the Blackwell Best Practice Guidelines on Publication Ethics were made public, promoted and followed by all Wiley-Blackwell journals; the guidelines are available at the Wiley-Blackwell webpage [22]. Common rules and guidelines are also available at the webpages of several international editor associations.

Having the largest number of members, the COPE is the most widely acknowledged organisation that provides guidelines to authors, editors and reviewers on issues of ethics. In its webpage it provides significant information on dealing with scientific misconduct and offers several other services such as newsletters, blogs, annual reports etc. In addition, all scientific misconduct cases and guidelines that have been discussed since 1997 up to date have been gathered in a database with a search engine. At the moment, this database contains more than 400 cases along with the advice provided by COPE for each case. For more recent cases of misconduct the database contains additional information on their course and outcome.

Furthermore, the COPE has designed flowcharts to help editors follow a certain Code of Ethics and put guidelines into practice in order to investigate cases of suspected misconduct. These flowcharts provide information on every type of scientific misconduct, such as plagiarism, duplicate publication, suspected guest, ghost or gift authorship etc. Publishers and authors have been extremely positive towards these flowcharts and encourage their use [23].

Apart from the guidelines provided by publishing houses and associations, editors can also take recourse to an international project named CrossCheck, a very effective tool for detecting plagiarism. CrossCheck powered by iThenticate, is a plagiarism screening service designed to help publishers verify the originality of the content submitted to them for publication. It allows publishers to ascertain the originality of the submitted manuscripts and helps them identify cases of misconduct. Participating publishers analyse submitted manuscripts with iThenticate

software, which checks submissions against millions of published research papers (the CrossCheck database), documents on the web and other relevant sources. Manuscripts with overlapping text are flagged to editors, who are able to further compare the documents in order to establish the reason for the matches [24].

During this process, the manuscript that has been submitted for publication is automatically compared to millions of other papers in the data base, providing the user with a percentage of similarity. Thus, it is easier to investigate and deal with certain issues such as plagiarism and self-plagiarism or even duplicate publication in cases where there is a very high percentage of similarity with another paper of the same author [25, 26]. Numerous publishing houses are already taking part in the CrossCheck project, such as Elsevier that has offered 9 million papers to the database [27]. Some of the project's reported negative aspects include limited access, system slowness, and staff time [28].

## 5. Conclusions

A simple inquiry with an internet search engine reveals that despite the steps taken so far editors and by extension publishing houses are not able to fully address the issue of scientific misconduct. Nowadays, there is a rich literature providing advice and general guidelines to authors and editors so as to foster ethical scholarly writing and publishing. However, according to research, a high percentage of journal editors internationally are not aware of the existence of these rules and guidelines or do not follow them [29]. Only a few researches and empirical studies have been conducted in order to estimate the percentage of unethical publications or investigate the behaviour of editors towards scientific misconduct. Identifying the publishing houses, editors and authors that continuously publish unethical papers and examining potential sanctions might help raise awareness within the academic and publishing community.

The entire academic and research community should maintain high standards in scientific research so as to preserve the integrity of science. Scientific work should be conducted responsibly and ethically. In a scholarly setting, knowledge should be produced by scientists who respect the intrinsic value of scientific knowledge and gain satisfaction from the quality of their research. Scholars are expected to contribute to the development, evolution, progress and dissemination of knowledge but at the same time they should also seek personal evolution and adopt moral values and practices. True scientists should not attempt to deceive others or themselves, mainly due to the fact that science is a moral phenomenon [1]. Thus, scientists should be primarily trained in understanding the nature and the meaning of science. Only ethical research and writing can lead to ethical publishing.

Apart from the unethical behaviour on the part of authors, journal editors are frequently confronted with editorial misconduct, a recent issue that has not yet been extensively researched [30, 31]. As a matter of fact, editorial misconduct is a rather hazardous behaviour that could compromise the integrity of science. Editorial misconduct could be defined as any type of bias (racial, national, religious) that could hinder the approval of a submitted manuscript. Confirmatory bias is a common type of misconduct where editors (or reviewers) decide on whether they are going to accept a manuscript based on the research results. As shown by William Epstein, a research with positive results has more chances to get published [13]. Consequently, all the existing associations that provide support and advice to editors should also monitor and control their behaviour [29].

Journal publications are expected to spread ideas, recognize and diffuse scholarly research. Publishing unethical work may lead to the dissemination of misleading and harmful information. In that respect, editors and publishers should re-examine their role and responsibilities towards scholarly publishing and the scientific community. There is an increasing need to raise awareness on the problems deriving from scientific misconduct in scholarly publishing. Furthermore, editors and reviewers should be supervised within the frames of editorial freedom, so as to eliminate any form of misconduct. Within today's constant increase in electronic information sources, peer-reviewed journals should offer high quality publications and provide the scientific community only with trustworthy and ethical researches.

**Acknowledgments:** I would like to thank my translator Mrs. Marilia Tilli who is always willing to offer her help and Dr. Maria Botti for urging me to participate at the International Conference on Information Law. I would also like to express my honest gratitude to Dr. Christina Banou, who inspired my love for science and supports my first steps.

## References

- [1] Zwart, Hub, *Professional ethics and scholarly communication*, available in: <http://www.filosofie.science.ru.nl/cv/prof%20ethics.pdf> (accessed in 12/3/2011).
- [2] Goodrum, Abby A. et al. (2001), "Scholarly publishing in the Internet age: a citation analysis of computer science literature", *Information Processing and Management*, No. 37, pp. 661-675.
- [3] WAME Publication Ethics Committee, *Publication Ethics Policies for Medical Journals*, available in: <http://www.wame.org/resources/publication-ethics-policies-for-medical-journals#eddecis> (accessed in 20/3/2011).

- [4] Pimple, Kenneth D. (2002), "Six Domains of Research ethics: a Heuristic Framework for the Responsible Conduct of Research", *Science and Engineering Ethics*, No. 8, pp. 191-205.
- [5] Public Health Service (1989), «Responsibilities of Awardee and Applicant Institutions for Dealing with and Reporting Possible Misconduct in Science», *Federal Register* 54, pp. 32446-32451.
- [6] King, Cynthia R., "Ethical issues in writing and publishing", in *Clinical Journal of Oncology Nursing*, available in: <http://www.ons.org/Publications/CJON/AuthorInfo/WritingSupp/Ethics> (accessed in 20/3/2011).
- [7] ISAJE, "Ethical practice guidelines in addiction publishing: a model for authors, journal editors and other partners", *International Society of Addiction Journal Editors*, available in: <http://www.parint.org/isajewebsite/ethics.htm> (accessed in 15/2/2011).
- [8] Albert, Tim, Wager, Elizabeth (2003), "How to handle authorship disputes: a guide for new researchers", *The COPE Report*, available in: <http://publicationethics.org/files/u2/2003pdf12.pdf> (accessed in 27/2/2011).
- [9] McKercher, Bob et al. (2007), "Why referees reject manuscripts", *Journal of Hospitality & Tourism Research*, Vol. 31, No. 4, pp. 455-470.
- [10] Keh, Tat Hean (1998), "Evolution of the book publishing industry: structural changes and strategic implications", *Journal of Management History*, Vol. 4, No. 2, pp. 104-123.
- [11] Banou, Christina (2007), "Publishing policy and content evaluation of medical publications: assuring the quality of printed material", *Proceedings of the 5th International Conference on Information Communication Technologies in Health*, Samos Island, July 2007, National and Kapodistrian University of Athens, Athens, pp. 334-40.
- [12] Powell, Walter W. (1985), *Getting into print: The decision-making process in scholarly publishing*, Chicago: The University of Chicago Press, pp. 72-78, available in: <http://books.google.gr/books?id=uZHr35XjFwIC&printsec=frontcover#v=onepage&q=&f=false> (accessed in 15/2/2011).
- [13] Bogdanovic, Gordana (2003), "Publication ethics: the editor-author relationship", *Archive of Oncology*, Vol. 11, No. 3, pp. 213-215, available in: <http://www.doiserbia.nb.rs/img/doi/0354-7310/2003/0354-73100303213B.pdf> (accessed in 13/1/2011).



- [14] Borkowski, Susan C., Welsh, Mary Jeanne (1998), "Ethics and the Accounting Publishing Process: Author, Reviewer, and Editor Issues", *Journal of Business Ethics*, No. 17, pp. 1785-1803.
- [15] Serebnick, Judith (1991), "Identifying Unethical Practices in Journal Publishing", *Library Trends*, Vol. 40, No. 2, pp. 357-372.
- [16] International Committee of Medical Journal Editors (ICMJE): <http://www.icmje.org> (accessed in 3/4/2011).
- [17] World Association of Medical Editors (WAME): <http://www.wame.org/>
- [18] International Society of Addiction Journal Editors (ISAJE): <http://www.parint.org> (accessed in 3/4/2011).
- [19] Council of Science Editors (CSE), available in: <http://www.councilscienceeditors.org/i4a/pages/index.cfm?pageid=1> (accessed in 3/4/2011).
- [20] The Committee on Publication Ethics (COPE): <http://publicationethics.org/> (accessed in 3/4/2011).
- [21] COPE, *COPE Best Practice, Guidelines for Journal Editors*, available in: [http://publicationethics.org/files/u2/Best\\_Practice.pdf](http://publicationethics.org/files/u2/Best_Practice.pdf) (accessed in 10/1/2011).
- [22] Blackwell Publishing, *Best Practice Guidelines on Publication Ethics: A Publisher's Perspective*, available in: <http://blackwellpublishing.com/Publicationethics/?site=1> (accessed in 15/1/2011).
- [23] Wager, Elizabeth (2010), "The Committee on Publication Ethics Flow-charts", *Chest*, No. 137, pp. 221-223, available in: <http://chestjournal.chestpubs.org/content/137/1/221.full> (accessed in 23/2/2011).
- [24] *CrossCheck Plagiarism Screening*, available in: [http://crossref.org/crosscheck/crosscheck\\_for\\_researchers.html](http://crossref.org/crosscheck/crosscheck_for_researchers.html) (accessed in 29/1/2011).
- [25] Meddings, Kirsty (2010), "Credit where credit's due: plagiarism screening in scholarly publishing", *Learned Publishing*, Vol. 23, No. 1, available in: <http://xa.yimg.com/kq/groups/18751725/1128775922/name/credits+where+credits+due+plagiarism.pdf> (accessed 19/1/2011)
- [26] Zhang, Helen Yuehong (2010), "CrossCheck: an effective tool for detecting plagiarism", *Learned Publishing*, Vol. 23, No. 1, pp. 9-14.
- [27] Elsevier, *Plagiarism detection*, available in: <http://www.elsevier.com/wps/find/editorsinfo.editors/plagdetect> (accessed 23/2/2011)
- [28] Council of Science Editors: Annual Meeting Reports (2008), "How Easy to Cheat? How easy to Uncover Cheating", *Science Editor*, Vol. 31, No. 6, available

in: <http://www.councilscienceeditors.org/files/scienceeditor/v31n6p186.pdf> (accessed 10/4/2011)

[29] Wager, E. et al. (2009), "Science journal editors' views on publication ethics: results of an international survey", *J Med Ethics*, No. 35, pp. 348-353.

[30] Teixeira, Aurora A. C. et al. (2010), "Who Rules the Ruler? On the Misconduct of Journal Editors", *Journal of Academic Ethics*, No. 8, pp. 111-128.

[31] Godlee, Fiona (2004), "Dealing with editorial misconduct", *BMJ*, Vol. 329, available in: <http://www.bmj.com/content/329/7478/1301.full> (accessed 10/4/2011).

# State-based internet censorship: direct or delegated practices and their effects on the free flow and future of the internet

---

---

Kyriaki Pavlidou

---

---

## Introduction

Internet featuring a great deal of information dissemination and interactive usage, with an estimated two billion number of active users around the world, still manages to keep its “magic”, while creating an unparalleled sense of freedom and power of unobstructed expression to its users or even non users. For how long though? Now that we are more than ten years into the Internet revolution [Palfrey, 2007], this is a question that is imperatively raised.

The Internet and wireless technologies have been heralded as vehicles of free expression and it has generally been thought that no government could control information on the Internet [Maurushat, 2008], hence the expression “the Internet interprets censorship as damage and routes around it”. However, this does not appear to be the case anymore. On the 22<sup>nd</sup> of last September 2010, Google finally came to acknowledge what transparency and privacy advocates criticised it for as well as what was being voiced long before among scientific communities, was estimated in various organizations reports or was even suspected by internet users: that Internet is as a fact being blocked, in other words it is being censored. With the so-called *Transparency Report*, an interactive platform that was launched as a deterrent to censorship<sup>1</sup>, Google attested that Internet traffic to Google sites is blocked and that government requests around the world are frequently made.

“One Internet is no longer there” [Bambauer, 2009]. The local nature or view of the Internet has changed, so that “one state’s Internet does not look the same as another’s” [Seltzer, 2008]. An increasing number of democratic and undemocratic states worldwide have already taken steps or have been considering doing so, through different legal or technical controls such as blocking Internet access, regulating content, or imposing digital filters. As a result, Internet looks different

---

1. Claire Cain Miller, The New York Times Bits, September 21, 2010, statement made by Niki Fenwick, a Google spokeswoman, on “Google Reports on Government Requests and Censorship”.

depending on our vantage point of access and the global flow of information is tempered by the activity of the censors.

For oppressive societies, the strongest form of the argument in support of online censorship is that censorship comprises “a legitimate expression of the sovereign authority of states or more simply [an] unalterable right of a state to ensure its national security” [Palfrey, 2007]. On the other hand, in democratic societies, the basis for Internet filtering or other content control relates to issues of copyright infringement, hate speech, sensitive historical facts, defamation, privacy protection or child protection [Dutton, Dopatka, Hills, Law and Nash, 2010].

Censorship in the net though, prompts legitimate and normative concerns the most straightforward of which involve civil liberties [Palfrey, 2007] such as the basic rights of freedom of expression and individual privacy. Moreover, it points out thorny topics in relation to international enforcement through direct or indirect control, as well as less evident issues like perception of the public, i.e. how transparent is for individuals to understand and realize that censorship occurs, or how free do they feel to express their opinions or make any kind of action on the Internet. Subsequently, although the Internet is generally seen as a “forum of free expression, in reality speech on the Internet is subject to unfettered censorship and discrimination at a variety of chokepoints” [Nunziato, 2009], while censorship around the world is usually a *fait accompli*, as far as users are concerned.

Filtering techniques have already progressed extensively. Internet experts claim now the appearance of second and third generation censorship methods; those methods create a legal and normative environment along with technical capabilities, while reducing the possibility of blowback or discovery even more [Deibert and Rohozinski, 2010].

Motives under these practices vary and come from different angles, political, economical, ethical, and technological. Censorship is an economic activity, according to some, which also bears political cost [Crandall, Zinn, Byrd, Barr and East, 2007]. For others “the actual result of censorship *ex ante*” cannot be foreseen and support of censorship is done in anticipation of increase in surplus afterwards [Depken, undated]. Either way, an ongoing greed for censorship is spreading over the internet in democratic and less democratic societies, reflecting on the flow of information and creating an ambiguous and less appealing Internet future to come.

## Defining Internet Censorship

“[...] When we attach a PC to the Internet, we might as well be wading through open sewers. Currently, many ISPs are allowing Internet traffic to flow through their systems completely unfiltered, which is akin to a water authority pumping out raw sewage to its customers to clean for themselves.” (ZDNet, 2004).

Internet censorship provokes certain confusion. Comparing the need for filtering of drinking water by authorities with the need for internet censorship is a good example of what internet censorship is actually not needed for. Internet filtering primarily on a state level is not an action willingly set in motion of those who wish to be filtered, as it is with water. People do not need “clean” Internet as they need “clean” water, and certainly they do not need someone to clean it for them. Internet it is not something that is piped into one’s home where it is passively consumed [McIntyre and Scott, 2008]. On the contrary it takes time, a minimum at least technical knowledge and effort, so, that Internet steps into someone’s house. Therefore, while filtering is increasingly normal, it should not be seen as natural [Bambauer, 2009].

When we refer to Internet censorship, we mostly end up using “Internet filtering” as synonymous with it. Internet filtering and blocking, Internet surveillance, net neutrality are the most commonly used expressions to describe the current concept of internet censorship.

Respectively, Internet filtering – in Palfrey’s wording – refers to the practice by which states restrict citizens from accessing or publishing certain information on the Internet. But should censorship be separated from surveillance? Internet surveillance refers to the means by which states record, listen in on, or track down conversations that take place over the Internet [Palfrey, 2007]. Internet filtering, yet closely related, is distinguished from internet surveillance; moreover, the manner and extent of censorship operations is easier as opposed to that of surveillance which is rather more elusive [Palfrey, 2007]. As it concerns the principle of network neutrality this one ‘holds that, in general, network providers may not discriminate against content, sites, or applications’ [Balkin, 2009]; in order to picture that concept, network neutrality “is about the rules of the road for Internet users, and about the relationship between the owners of those roads and the users. Government is asked to make a decision as to which users have priority and whether road charging should be introduced ostensibly to build wider and faster roads in future” [Marsden, 2009].

All these terminologies, similar to each other, still differ in certain points of meaning. From our point of view internet filtering and surveillance imply the technology factor existing and have a more technical dimension, while network neutrality implies mostly the human factor behind the web activities and underlines the importance of a more values-based approach. However, according to a scholar’s intriguing aspect, filtering is shorthand for technology that implies a choice on the part of the user, so it is preferable to talk in more neutral terms using “blocking” or even “censoware” instead of filtering, which are beyond user

control [McIntyre and Scott, 2008]. In the present paper when we refer to state-based internet censorship practises we focus mainly on filtering terminology.

State-based internet censorship should be further separated from private-initiated censorship. The latter may occur either with the cooperation of the government for state purposes or it may also occur exclusively in favour of private sector's interests<sup>2</sup>.

Internet censorship though is not to be fully comprehended yet. To understand this phenomenon we should refer to the "end to end argument" or principle of "end-to-end neutrality" [Zittrain, 2002], which consists a central design principle of the Internet. According to it, internet protocols are designed to execute relatively simple packet-forwarding function moving data packets from the sender to the receiver without regard to their content or security. As a result, the "intelligence" of the network is placed in the middle of it rather at the end-points [Palfrey, 2007] often referred to as "the edges" of the network. As a result, the other functions are supposed to be performed at their networks or computers, empowering in this way the end-users of the network [Bendrath, Mueller, 2010]. Internet censorship violates the end-to-end principle of network design, by handing control in the middle of the network rather than at the user level<sup>3</sup>.

---

2. A common example refers to institutions which enable filtering systems in their computer networks in order to prevent the recreational use of workplace computers. But is it the same when companies prohibit the use of social networks for example to their employees during their job? See the recent court decision 32/2011 of Athens First Judicial Court regarding the case, available at <http://www.enet.gr/?i=news.el.article&id=268598> /accessed 10.04.2011. Another version of private-initiated censorship concerns the filtering software which is activated in personal computers with the approval, consent and knowledge of the user; in this case when the user chooses to filter his own individual computer no internet censorship is implied, except from those cases of censorship when it is implement by one user at the expense of other co-users of the same computer.

3. The relation between the end-to-end principle and internet censorship is pictured vividly in the following everyday-life scenery. Let us imagine at first a daydreaming postal worker, walking on foot delivering letters and riding his bicycle, hoping on and off in front of every address he has a mail for. In sequence to that reads Lawrence Lessig's well-turned metaphor: "Like a daydreaming postal worker, the network simply moves the data and leaves interpretation of the data to the applications at either end. This minimalism in design is intentional. It reflects both a political decision about disabling control and a technological decision about optimal network design" [Bendrath and Mueller, 2010]. Now let us imagine, urges us Bendrath and Mueller to their exact words, "a postal worker who is not daydreaming, but instead: Opens up all packets and letters; reads the content; checks it against databases of illegal material and when finding a match sends a copy to the police authorities; destroys letters with prohibited or immoral content; sends packages for its own mail-order services to a very fast delivery truck, while the ones from competitors go to a slow, cheap sub-contractor [...]. Shall

## Means and Locus of Internet Censorship

When it comes to the different means of internet censorship, the digital age has brought a new way of censorship; that is to say for the first time *technology can be used as a means of censorship*. For the first time, the instruments of control can be integrated with the medium [Chalaby, 2000].

Advanced information technology or legal mechanisms and soft controls are what a growing number of states around the world uses in their attempt to control the global flow of information [Palfrey, 2010]. When state authorities crucially depend on the intervening medium of technology to impose their desirable measures, then medium-integrated mode of control is the case. On the other hand, when state regulators have immediate access to internet content, then we mostly refer to legally and technologically combined strategies which can be enacted over the net by state ascendance.

Rewarding the various methods of internet censorship, our interest is focused on the mainly state-based censorship techniques which are presented (see bellow). The basic approach in which internet filtering occurs is technical blocking, search results removal, take-down of websites and induced self-censorship.

### i. Medium-integrated means of online control

The most apparent mode of online control is through the use of technology [Palfrey, 2007]. Before filtering occurs there is a two-step process involved, which breaks down to the use of *rating* and *filtering* software [Chalaby, 2000]. Rating consists of classifying web content according to the different categories such as violence, nudity and so forth and it is followed by filtering [Chalaby, 2000]. The assortment of web collection is based on filtering software or different rating platforms (such as the former Platform for Internet Content Selection {PICS} or the current Protocol for Web Description Resources (POWDER) along with others).

A state wishing to filter its citizens' access to the Internet has several initial options, but three of them are most commonly used in order to block access to Internet sites when direct jurisdiction or control over websites is beyond the reach of their authority. Those techniques are IP filtering, DNS filtering and URL blocking

---

we imagine also that the postal worker could do this without delaying or damaging the packets and letters" [Bendrath, Mueller, 2010] compared to his (former, now fired) daydreaming colleague. Thereupon, Internet censorship is like the slipped postal worker, as it violates this end-to-end principle of network design, by handing control in the middle of the network rather than at the user level [Palfrey, 2007].

using a proxy or keyword searching, which are accordingly used to block access to specific domain names, IP addresses or WebPages.

Respectively, as far as *Internet Protocol (IP)* filtering concerns, the state places special code on computers that lie between the individual end-user and the broader network [Palfrey, 2007] so that certain data packets with a destination or source address on this list are blocked from reaching their destination, are dropped by the routers within ISP networks [Brown, 2008], or are used so that information about the content or the creator of the requested address is obtained<sup>4</sup>. On the other hand *Domain Names filtering* or poisoning, refers to manipulating DNS information, which involves falsifying the response that is returned by a DNS server [Dutton, Dopatka, Hills, Law and Nash, 2010]. Finally, *keyword blocking* is a more advanced technique that a growing number of countries are employing. URL or keyword blocking occurs when the search engine of a web browser which is connected to certain blocking software *either* blocks searches involving blacklisted term *or* filters content; this filtering procedure is based more on the words found within the URLs addresses, which are provided by the software's rating system, rather than on the potential of a dynamic content analysis.

As it concerns removal of search web results, this method is used in order that undesirable websites are omitted from search results; that is to say, finding the sites more difficult is preferred to blocking access to the targeted sites (source, ONI).

## ii. Legal and technical-integrated means of online control

The manner, in which legal and technical-integrated means of online control is exercised, varies. In order for states to carry out online censorship effectively they sometimes take control into their own hands by erecting technological or other barriers within the state's confines to stop the flow of bits from one recipient to another private party [Palfrey, 2007]. However, it is possible for a state to turn to private parties in order to carry out online control whenever the state is unable to carry out filtering on its own [Palfrey, 2007]. Those private intermediaries are quite often corporations chartered locally or individual citizens who live in that jurisdiction whose services connect one online service to another [Palfrey, 2007].

State-based censorship is localized at different network nodes, performed through different private intermediaries of control (Internet backbone, ISPs, In-

---

4. Brown I. (2007), *Internet Filtering - Be Careful What You Ask for. Freedom and Prejudice: Approaches to Media and Culture*, Kirca S., Hanson L., eds., 74-91, Istanbul: Bahcesehir University Press (2008); the method of "blocking traffic to and from lists of websites specified by their Internet Protocol address (a numerical identifier such as 128.16.64.1) is characterized as the simplest filtering mechanism".



stitutions, PCs) and succeeded as depicted in the different portrayals of social life. In particular ISPs, which are characterized as the most critically situated point of control on the Net, can direct the flow of the Internet in multiple ways; they may be asked to prevent subscribers from linking to particular sites, take down “objectionable” sites hosted to their servers [Demont-Heinrich, 2002] or act like gatekeepers monitoring control on certain portals. Web-based services on the other hand may be required to hand down to state agencies the email addresses or even email content of their users; online telecommunication services may be forced to wiretap online conversations in voice or in the form of instant messages, but in this case it is more likely to be confronted with internet surveillance; social networks may be asked to provide all sort of information that is uploaded to their servers by end-users. Non-governmental organizations and religious leaders may be required to register before using the Internet to communicate about the topics that they work on [Palfrey, 2010]. Schools may be obligated to filter their networks, or install filtration software on each individual computer they provide (source, ONI)<sup>5</sup>. Owners of cyber-cafes may be called upon to report on the identity of a certain Web surfer who used a given PC during a given time interval [Palfrey, 2007], or may be forced upon state order to even have a certain furniture arrangement in their cafes halls<sup>6</sup>.

Those practices build up a suspicious environment for the user which eventually may lead to a form of self-censorship. This induced censorship of oneself is encouraged little-by little in the scope of national or international legislation and state enforcement, through the promotion of social norms or with the use of intimidation methods or informal commendations for compliance with certain domestic habits and practices. The blocking of web pages or the constant feeling of users that they are subject to web content restrictions or that they should be, may be intended – in Palfrey’s well-aimed words – to deliver a message to users that state officials monitor Internet usage, making it clear to them that “someone is watching what [they] do online” [Palfrey, 2010]. This perception that the government is engaged in the surveillance and monitoring of Internet activity, whether accurate or not, provides according to ONI another ‘strong incentive to avoid posting material or visiting sites that might draw the attention of au-

---

5. For instance in Greece it is implemented in school networks the so called “Greek School Network Web Filtering” service (<http://www.sch.gr> in association with [www.safeline.gr](http://www.safeline.gr)).

6. Such an example refers to Egypt, where computers at internet cafes were asked to be placed in a circle arrangement with the screens facing the café owner’s desk so that the owner could easily keep sight of all users’ online activity. [Source, documentary “Reportage Without Frontiers: The Rebels of the Internet” (original title in Greek, “Περιοπάζ Χωρίς Σύνορα: Οι Αντίρρες του Διαδικτύου”, aired 28/03/2011 in National Greek Television Network, NET), online accessible at <http://www.rwf.gr>].

thorities'. As a result, soft controls and regulative state improvisations on legal grounds point at more and more incidents of self-censorship within the Internet.

However, medium intergraded or legal and technical integrated methods are considered to be outdated, as new means of censoring the Net have in sight featuring second- and third-generation techniques. According to the most recent documentations and scholar approaches, national filtering schemes as those of China represent the first generation ones, while second- and third-generation filtering technologies are more subtle, flexible, and even more offensive in character. These next-generation techniques "employ the use of legal regulations to supplement or legitimize technical filtering measures, extralegal or covert practices, including offensive methods, and the outsourcing or privatizing of controls to "third parties," to restrict what type of information can be posted, hosted, accessed, or communicated online" [Deibert and Rohozinski, 2010].

Examples of next generation techniques include "the infiltration and exploitation of computer systems by targeted viruses and the employment of distributed denial-of-service (DDoS) attacks, surveillance at key choke points of the Internet's infrastructure, legal takedown notices, stifling terms-of-usage policies, and national information-shaping strategies" [Deibert and Rohozinski, 2010].

It is also likely that, while wandering on the Net, we might have already come across certain feedback suggesting that the website is not available ('file not found') or that access has been inhibited by some technical problem (eg 'connection timeout') [McIntyre and Scott, 2008]. This might be a form of new generation internet censorship, too; in particular, it is possible that the authorities may use this method of "error pages" in order to block some websites of opposition political groupings, media or human rights organisations, that may have deemed unacceptable by them, "deflecting in this way criticism and allowing themselves to claim that they are not censoring Internet content" [McIntyre and Scott, 2008]. If a more transparent and accurate message, 'access blocked by government order' was given instead of an innocent error page, the former allegation of the authorities could not easily stand [McIntyre and Scott, 2008].

Moreover, one filter that has become commonplace in many countries and their censorship reflex actions, is the so called "just-in-time" filtering. This filtering technique relates to the phenomenon of a state blocking particular types of speech or other forms of online action "at a sensitive moment, rather than in the same, constant way over time" [Palfrey, 2010]<sup>7</sup>. Libya is a representative ex-

---

7. Palfrey J. G., *Local Nets on a Global Network: Filtering and the Internet Governance Problem*. (Chapter in *The Global Flow of Information*, Jack Balkin, ed., Forthcoming), Harvard Public Law Working Paper No. 10-41, 2010, p. 12: "For instance, the Chinese state blocked applica-

ample; in the most recent political events that conducted in Libya, the government, while routing all wire line Internet connections into the inland through state-owned telecommunications authority and without using authorized private ISPs, was consequently loaded with a serious advantage over controlling Internet on a state base. Therefore, on March 4, 2011, “the authority flipped the “kill switch”<sup>8</sup>, which prevented persons in government-held territory such as Tripoli from receiving messages of support for the revolution from the outside world, and slowed images of the revolution from getting out” [Travis, 2011]. In Egypt, the authoritarian state regime virtually shut down Internet connections to the country [Chen, 2011] from midnight 27/28 April till 2 February 10:30 GMT [Comninos, 2011]<sup>9</sup>.

---

tions such as Twitter and YouTube at the time of the 20<sup>th</sup> anniversary of the Tiananmen Square demonstrations in June 2009”.

8. The similar Internet “kill-switch” method was also used in Tunisia during the political protests of January 2011. Thomas M. Chan, Governments and the Executive “Internet Kill Switch”, IEEE Network, March/April 2011, p.p. 1-2: “As protests escalated, the government took more actions to selectively block Internet sites but did not shut down Internet services completely like Egypt. The Tunisian government reportedly blocked news sites and political blogs, and started to arrest bloggers. Even more extreme, the Tunisian Internet Agency was suspected of injecting hidden JavaScript on certain Facebook pages to steal login passwords”; accordingly, Comninos A., Twitter revolutions and cyber crackdowns (subtitled) User-generated content and social networking in the Arab spring and beyond Association for Progressive Communications (APC), 2011, p.10: “[...] The Tunisian Government’s approach was far more advanced and involved the theft of user-names and passwords for Facebook, Twitter and online e-mail accounts like Gmail and Yahoo!. This was achieved through the injection of phishing scripts into the content of these pages before being sent to the end-user.”
9. Cheng Gr., Cohen M., Green J., Oliveira C., Stadnyk M.&I. Deyrup, Director, The Harvard Law National Security Research Group, Responses to Questions posed by CNAS or International Law & Internet Freedom, p.p. 1-26: “[...] in Egypt, [...] social media is playing an important role in sparking and coordinating protests in the region. Facebook groups like “We are all Khaled Said” offer support videos, slogans, news reports, and cautionary advice. On January 25, 2011, reports began trickling out that Twitter and Facebook – key tools – were being blocked. Google worked with Twitter to develop a bypass solution, the “speak-to-tweet” phone numbers: on January 31, 2011, they allowed Twitter users to create posts via phone call. Soon after Twitter and Facebook were taken offline, by January 27, 2011, Egypt then entirely shut off the Internet. Renesys claims that this occurred via shutdowns of the “big four Egyptian ISPs”: “Link Egypt, Vodafone/Raya, Telecom Egypt, [and] Etisalat Misr.” It appears that “each service provider approached the task of shutting down its part of the Egyptian Internet separately”, as if ordered by phone. This move, asserts Renesys, is unique in its scope: the Tunisian and Iranian blockages were partial or targeted. One ISP—Noor Group— was not shut down in this initial order. Renesys speculates that the government left Noor up and running because they host the Egyptian Stock Exchange. By February 2, 2011, Internet access—and access to Facebook—was restored.”

## Concrete systems and Effectiveness

“If Internet filtering were stock”, says Bambauer, “one would be well-advised to buy it; on-line censorship is on the march, in democratic states as well as authoritarian ones”. An increasing number of states around the world take part in censoring what their citizens can see and do on the Internet. The People’s Republic of China was among the first to implement national filtering systems at the backbone of the country’s Internet, popularly referred to as the “Great Firewall of China” and had thereby heralded a different era for the future of the Internet. It has thus even been accepted as to “to have created the first truly 21<sup>st</sup> Century censorship regime, a regime that could plausibly be modelled in societies that are otherwise democratic” [Fish, 2009]. However, while the “Chinese-style” [Deibert and Rohozinski, 2010] of Internet censorship receives considerable attention and acknowledgement, censorship in a range of democratic and undemocratic states worldwide is largely ignored by the majority [Bambauer, 2009].

China may have been the first to have implemented extensive controls over the information that their citizens could access, but certainly it was not the last one as it became a paradigm of Internet censorship ever since for other countries that follow at her wake. Many countries around the world have already taken and continue to take heavy measures on the Web while the number of states implementing those kinds of technologies is growing over time, as this trend has been emerging since at least 2002 [Palfrey, 2010].

Existing filtering regimes around the world are well-documented<sup>10</sup> [Palfrey, 2010]; only in 2007, ONI recorded 41 countries constructing defensive perimeters by building firewalls at key Internet choke points so that access to undesirable content is denied to users [Deibert and Rohozinski, 2010]. In addition, in the Government’s Request Section at Google’s Transparency Report, it may be noticed that 39 countries have requested for specific content to be removed or information about users, using certain Google’s services or products, to be provided (it is noticeable that Iran as well as Saudi Arabia, while implementing extensive filtering systems, are not listed notwithstanding among the countries in the Google’s Transparency Report table).

Control varies over different forms of content, with most prominent of all, the one related to blogs, social networks and NGOs. However, besides those, control

---

10. Documentation is based mostly on the work of OpenNet Initiative and Freedom House with its Global Index of Internet Freedom [Dutton, Dopatka, Hills, Law and Nash, 2010] as well as on the activities of other organizations such as Reporters Without Borders and Internet Watch Foundation (IWF).

is not limited to censorship, but takes an upsetting step towards various personal targeted threats. The most extensive of those involve the arrests of bloggers and Internet users; this practice has taken a dramatic toll regarding Internet's latest facts; "in particular the Committee to Protect Journalists found that only in 2008, there were, for the first time, more jailed 'cyber-dissidents', such as bloggers, than traditional media journalists" [Dutton, Dopatka, Hills, Law and Nash, 2010].

The intention to censor the Web is a given among various states; what differs among them, democratical or non-democratical ones, is *the content* they target, *how* precisely they block it and in *what* extent citizens get involved in the choice and decision making [Bambauer, 2009].

States, which use *direct control* in order to restrict content, impose legal force on intermediaries; on the other hand, regimes of *delegated censorship*, which do not operate the Internet infrastructure directly, control nonetheless what may be seen there by implementing indirect filtering through legal pressure upon those who search or index websites [Seltzer, 2008]. The first category of direct exertion, where states interfere in the backbone of the Internet on a country level, includes a relative handful of countries [Seltzer, 2008] such as it is China, Iran and Saudi Arabia.

The "rise of the Chinese Communist Party (CCP) brought with it the continued ideal of control over the dissemination of works and ideas" [Maurushat] and short after an entire censorship empire started spreading around the Chinese hectares of fictional Internet land. The sophisticated Internet censorship system in China – with a number of about 110 million users as reported in 2005 [Deva, 2008] – works through nine Internet Access Providers licensed by the government, which provide international network access to regional Internet Service Providers [Brown, 2008].

China censors<sup>11</sup> a wide range of political and religious dissent and human rights activism through her "Great Firewall" [Seltzer, 2008] in addition to most forms of publications and massive media that are considered to be a threat to the governing regime [Maurushat, 2008], violating in this way freedom of expression

---

11. In January 2010, there has been a significant change concerning Google's relationship with China. See, Dutton, Dopatka, Hills, Law and Nash, 2010, p.p. 62-63: "Google continued to auto-censor results on Google.cn until January of 2010 when the search engine announced that the company, along with at least 20 other large corporations, had faced sophisticated cyber-attacks originating from within China. These attacks lead to the theft of intellectual property for Google and the unauthorized access to the e-mail of dozens of human rights activists. Consequently, Google announced that it would stop censoring its search results on Google.cn and operate an unfiltered search engine, even if this meant closing its offices in China".

and other civil rights. Those sweeping restrictions, against information access may involve more than freedom of expression though. According to the interesting remark of Alana Maurushat, regarding the case of SARS, "China has a long-standing tradition of curtailing news deemed harmful to society and to China's image in order to reduce of public fear and to lessen economic damage in the region". So based in the above rationale, it negatively strikes us, that China does not hesitate to take even the price of blocking timely information that may have repercussions for the health and welfare of individuals [Maurushat, 2008]<sup>12</sup>.

However, in our point of view, health and welfare are not what is being at stake through these practices; these are side effects in a battle against what Fish claims to be the actual "underlying purpose of the Great Firewall"; and that is public discourse [Fish, 2009]. In Fish's accurate words, "the CCP does not desire to make any one piece of information completely inaccessible, as it knows that is impossible and that those heavy-handed attempts to restrict the Internet more thoroughly will harm certain sectors of the economy. Instead, the CCP seeks to control the flow of stories and information on the Internet by both promoting self-censorship and using its control over the broadband network to prevent potentially damaging information from bubbling up to the e-public's attention in the way that "viral" stories and videos so often do. In this way the CCP can control public discussion while still allowing its citizens substantial access to the wonders of the Internet" [Fish, 2009]. This well described underlying purpose is also detected, in our view, among other authoritarian or not filtering regimes worldwide.

Iran operates a similar to China extensive filtering system, requiring ISPs to block access to over 10 million websites [Brown, 2008], sometimes by blocking unexceptionally a cluster of permissible content deemed nearby an impermissible network standpoint [Palfrey, 2010]. More recently, Iran has taken further measures by qualitatively reducing the speed of international connections to 128kbps, so that blocking access to high bandwidth video streams could work effectively [Brown, 2008].

Saudi Arabia also implements one of the most far-reaching and longest-running filtering regimes while it routes all Web pages through a government proxy. Internet access to citizens was only introduced after many years and only when the state authorities were comfortable that this could be done in a manner that would not violate "the tenants of the Islamic religion or societal norms" (source, Internet Service Unit). In reason of that, the so-called Internet Services Unit was

---

12. Indeed, there are three specific areas, the argument goes on, "where censorship and a lack of accurate information distributed in a timely manner have had unrefuted consequences in China in recent history: AIDS, SARS and Avian Bird Flu", Maurushat A., Anti-Censorship, Benevolent Payloads and Human Rights, UNSW Law Research Paper No. 2008-60, 1-24.

activated under the directions of the government of Saudi Arabia so that it can oversee and filter or block pages of “an offensive or harmful nature to the society” (source, Internet Service Unit). At the same time, the state raised the argument that a state preserves the “right to protect the morality of it’s citizens” [Palfrey, 2007] and impressively justified this argument in support of censorship on the Web – otherwise benignly referred to as “usefulness of filtering” in the Internet Service Unit webpage – as a spiritual command deriving from the holy writings and finding a further confirmation to some sporadic and selectively scientific studies provided<sup>13</sup>.

Apart from the authoritarian filtering regimes to countries around the world, it is declared true that content control measures have become more prevalent [Dutton, Dopatka, Hills, Law and Nash, 2010] in many countries with democratic political systems and constitutional guarantees of protection of civil rights. In this second category of delegated censorship, we suggestively refer to Germany and to Australia’s unsuccessful attempt to establish online censorship through legislative mandate.

In Germany, a localized version of multinational search companies, such as Google responds to national requests by changing the content provided, so that if someone, while being in Germany, types for instance “http://google.com” into their web browser, they will be redirected to google.de, based on Google’s geolocation of the IP address from which the requested search was attempted. Pre-designated access though with forced redirection to localized version is also followed by curtailed search results. In addition, in Google’s Transparency Report, Germany appears to have the most voluminous action for the year 2010 among all other European countries, with a total number of 2199 data and items removal requests resulted from court orders that related to defamation in search results; in addition Germany is claimed to be the first European country along with France to impose restrictions on Nazi and other materials hosted overseas [Brown, 2008]<sup>14</sup>.

---

13. See Internet Services Unit, King Abdulaziz for Science and Technology, <http://www.isu.net.sa/saudi-internet/content-filtrng/filtrng.htm> / accessed 31.03.2011: “God Almighty directed humanity in the Noble Qur’an in the words of His prophet Joseph: “He said: My Lord, prison is more beloved to me than that to which they entice me, and were you not to divert their plot away from me I will be drawn towards them and be of the ignorant. So his Lord answered him and diverted their plot away from him, truly, He is the All-Hearer, the All-Knower” [the underlining to be within the text] Yusuf(12):33 34”.

14. A federal government youth protection agency in Germany, named BPjM, sends also URLs for sites that contain content that violates German youth protection law, like content touting Nazi memorabilia, glorification of violence, extreme “pornographic writings” or incitement, and those search results are being removed from google.de (Google- Deutschland), as both

Australia on the other hand, has dragged worldwide attention, when it decided to “implement Internet censorship using technological means, to mandate filtering legislatively and retrofit it to a decentralized network architecture” [Bambauer, 2008]. With that decision, Australia opened the way and marked a shift by Western democracies towards legitimating Internet filtering, without taking under consideration the alternatives available to combat undesirable information [Bambauer, 2008]. Australia’s Liberal Party ultimately, failed to create an Internet censorship, according to recent reports, demonstrating in this way that democracy can win over governmental control, once is consolidated and competitive, “with many viable parties and powerful anti-censorship constituencies” [Fish, 2009].

### **Inadequateness of Censorship Technologies**

Internet filtering and blockage mechanisms to control the Internet lack in precision and accuracy, are crude and ineffective [Brown, 2008], therefore being imperfect in general they are circumventable and can be easily evaded.

This happens, as citizens with technical knowledge can generally outsmart filters that a state has set in motion; as a result very rarely does any state manage to achieve complete filtering on any topic [Palfrey, 2010]. Pages removed from search results can be accessed with just a little effort as long as someone knowing a link decides to bypass the searching option and navigate directly to the site’s address. Likewise users who want to access blocked sites can do so, by using overseas Web proxies or intermediate machines that retrieve Web pages on behalf of them [Brown, 2008] or peer-to-peer systems or single proxy machines in order to enhance privacy protection or even activate technology that will override governmental restrictions measures. As an alternative, users are also able to use their own Virtual Private Networks (VPN) as a built-in escape valve in order to have access to a faster, unfiltered Internet [Fish, 2009]. Finally, it is quite possible for someone to still see the full generic set of results and to have full access to the removed sites as far as he forces a search engine to the generic.com-based pages rather than the localized ones [Seltzer, 2008].

---

pro-Nazi content or content advocating denial of the Holocaust are illegal under German law (source, Google Transparency Report). Searching from Germany for the photos of the Abu Ghraib prisoners posted to Rotten.com will return a depauperated set of results, due to reported illegal content and followed by the redirection to ChillingEffects.org after the phrase “Aus Rechtsgründen hat Google 8 Ergebnis(se) von dieser Seite entfernt. Weitere Informationen über diese Rechtsgründe finden Sie unter ChillingEffects.org”. See also Seltzer, 2008; when Wendy Seltzer wrote her paper she reported 23 results removed, during the same search, Seltzer, 2008, p.



Subsequently, a country that proceeds to filter the Internet “must make an “over-broad” or “under-broad” decision at the outset” [Palfrey, 2010]. That is to say, due to the widely extended cyber environment of seamless flow including billions of web-pages and other media, filtering of this huge material available on the Internet is made impractical and the least effective most of the times, while identification or targeting of one specific web-page for instance is unattainable.

The filtering techniques being extremely imprecise will either filter too much or too little Internet content or may block access to large amounts of legitimate material. In this case, filtering regimes will have to deal with underblocking or over-blocking results.

Underblocking refers to the failure of filtering to block content targeted for censorship, while overblocking stands for those cases when filtering software filter or block content, that they do not intend to block at the first place; this occurs as Internet content is too diverse to be classified and filtering operates most of the times by key words and are therefore unable to take into account contextual information in the process (source ONI). Because Web servers typically host many or sometimes thousands of sites, blocking one of them translates into blocking all the sites hosted on that server<sup>15</sup>. As a result, filtering technologies, being vague, imprecise or even incapable of any rating reasoning, they block incoherently large quantities of information that may be suitable and legal for all users, while even sites which have “no affiliation with the offending material may find themselves blocked if the common but crude approach of IP address filtering is used” [McIntyre and Scott, 2008]. The American Civil Liberties Union (ACLU) found that the use by someone of the consecutive letters ‘s’, ‘e’, and ‘x’ in a row, while wandering on search machines, may block sites which contain words such as ‘Mars exploration’ [Chalaby, 2000]<sup>16</sup>.

However, except from IP address filtering, overblocking can also occur because of DNS poisoning, as it can block access to non-Web services outside the targeted domain region, while same overblocking results occur in merely keyword filters

---

15. A good example is given by Palfrey who argues that “states make blocking determinations to cover a range of Web content, commonly grouped around a second-level domain name or the IP address of a Web service (such as <http://www.twitter.com> or 66.102.15.100), rather than based on the precise URL of a given Web page (such as <http://www.twitter.com/username>), or a subset of content found on that page (such as a particular image or string of text)” [Palfrey, 2010].

16. Another example is given by Brown, who argues that in 2003, when the Indian government ordered ISPs to block access to a specific Yahoo! Group, access to the entire domain was simply blocked, cutting access to around 12,000 groups (source Deibert and Villeneuve, 2005).

implemented by government routers, based on the lists of forbidden keywords, such as Cleenfeed in the United Kingdom [Brown,2008].

## A Matter of Legitimacy

In traditional censorship of books for example, if a government wishes to prohibit access to certain books, it follows a public legislative process, which involves elected representatives in the making of rules for enforcement by public officials [McIntyre and Scott, 2008]. “Legitimate censorship is open, transparent about what is banned, effective, yet narrowly targeted, and responsive to citizens’ preferences” [Bambauer, 2009].

However, the above presented inherent flaws of internet filtering and blocking software risk both to the efficiency and accountability among others equally important common features of the different technologies that are used. Overblocking and underblocking filtering practices, answer the question of the presumable *effectuality* and *openness* of filtering in a negative way, i.e. why access of certain information is being restricted, is not commonly answered by the states. *Narrowness* of restricted content fails to succeed either; overinclusiveness with overbroad outcomes of innocent content being blocked or underinclusion with underbroad filtering systems which fail to block proscribed material [Bambauer, 2009], are the two sides of the coin.

Similarly most of the times, in addition to the above, what is pointed out is the issue of transparency. When it comes to the filtering mechanisms, it is possible that the affected user will receive an email or notification or will be sent a summary that a webpage is out of reach due to blocking. However, filtering and blocking is often opaque [McIntyre and Scott] and lacks a great deal of transparency and disclosure of blocked material, methods and frequency of blocking tactics. Browsers who see pages disappear are likely to see the author’s explanation, whereas when sites are blocked at a search-engine level, it is up to the search providers to notify their end-users [Seltzer, 2008].

Most of the times, though search engines hold back on this information and leave searchers unaware that filtering is in operation and that “a site they never saw is gone” [Seltzer, 2008]. Among the major search engines only Google gives indication of search results removals due to legal demands, sending removal requests on to the Chilling Effects Clearinghouse<sup>17</sup> where the searcher can see the content

---

17. Chilling Effects Clearinghouse is a joint project of the Electronic Frontier Foundation and Harvard, Stanford, Berkeley, University of San Francisco, University of Maine, George Washington School of Law, and Santa Clara University School of Law clinics, available at <http://www.chillingeffects.org>.

of the pages that is missing as well as the identity of those responsible. On more recent events, Google as mentioned above has also launched Google Transparency Report, giving further access to every user<sup>18</sup>.

Last but not least follows the issue of legitimacy for states, which implement filtering regimes, as well as the matter of participation of citizens in the decision making process [Bambauer, 2009]. Therefore accountability is reflected in the extent to which filtering is being implemented with the consent of public actors and legal rules. On the other hand, some may argue that technological control through filtering is applied automatically, so there is no much space for human intervention and no scope for argument. We address this allegation just further down; we would like to argue here, though, that even if technology in its automatic enforcement does not exercise discretion against users, depending on code by nature [McIntyre and Scott, 2008], it still raises issues of accountability as far as it is used at the expense of public discourse and as long as it oppresses public discourse. When basic human rights are jeopardized, no position in favour of censorship can stand based on the fact that we are all – in technological terms – equally censored.

### **Do we have to reassess the matter of censorship all over again?**

Sigmund Freud made the following observation in 1933: “What progress we are making. In the Middle Ages they would have burned me. Now they are content with burning my books”. Have we learned nothing since Freud made this observation in 1933, asks Professor Brown eminently [Brown, 2008]; have we only gone from burning books to “burning” e-libraries?

It is not the flames like in the Inquisition that “now suppress information but invisible and anonymous digital codes [...] that operate behind the screens, not in public places, and end-users may not even be aware of their presence in software packages”, argued Chalaby 11 years before [Chalaby, 2000]. In the Middle Ages, image and its force were used to inculcate values, intimidate, and “deploy before all eyes an invisible force” [Foucault, 1977 in Chalaby, 2000]. “If digital technologies are allowed to become widespread and sophisticated instruments of censorship, they could constitute an invisible, timeless and faceless way of con-

---

18. Among countries operating extensive filtering regimes Saudi Arabia, via Internet Services Unit notifies users when access to certain pages is blocked [Brown, 2008] and provides block/unblock requests forms.

trolling discursive flows in the digital age”, predicted Chalaby as well [Chalaby, 2000]. Or could they not?<sup>19</sup>

What was aptly described in 2000 by Chalaby, is in our point of view, only the one cast of a batch that has too many players, too much profit, too much controversy and too much of a future ahead of it until we end up telling that code is actually the spectre of Internet. Nowadays, code may be masterfully used by states either by implementing it or by threatening for its enforcement and it may well bear a new symbolism for the Internet era, i.e. that we should be intimidated by technology as we were intimidated by the medieval rituals. Image may not be used the way it did, but instead it is rather intentionally avoided; it cannot drag the attention of all eyes at once that easily; it cannot cause fear on the extent that it used to. Yet the image is still at stake; the image that we do not get to see. Everyone uses the Internet but hardly few of the broadband internet users know exactly what they actually use and what they are deprived from in the process. However, eleven years after Chalaby’s remarks, what current documentations and scholar approaches give precedence to over technology itself, are the new generation censorship technologies based on government forces as well as the reflex reactions to dissents combined with the extensive self-censorship inducement cases<sup>20</sup>.

McIntyre and Scott have an interesting argument to add. They claim that using the internet with the implication that we may freely do whatever it is technically possible to do and with no necessity of moral engagement in our activities we may be robbed “of moral agency or responsibility”. If such consequences, they say, “were to follow through into wider patterns of social interaction, the con-

---

19. On the nature of the Internet, the questioning that has arisen is whether or not internet technology will turn up to overrule traditional narratives of legitimacy in the long run or not; in other words, will code be the law? We will hold back to that thought, as any further analysis is beyond the scope of this paper. A first answer though has already been given by professor Lawrence Lessig; he argued that “code is law” and with this celebrated claim he dramatically highlighted a future where the potential of software architecture will substitute for law in the control of behaviour. See McIntyre T. J. and Scott, C.D., *Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility. Regulating Technologies*, Brownsword, R., Yeung, K, eds., Oxford, Hart Publishing, 1-15, 2008.

20. Then, why are we left back to talk only about technology? It looks like when we talk about it, what we may fear that will happen in the next five minutes may have happened ten minutes before. What we may picture to come in the next decades, may be happening as we speak. So, it is fruitless to seek liability merely on technology. After all what lies underneath is the human factor, as “every technology is extension of the intuition of the man, of the limits of the man himself” [Corasaniti, 1996 in Cammarano, 2002].

sequences for responsibility, and for social ordering generally, of such low trust mechanisms of control might be troubling" [McIntyre and Scott, 2008].

So do we have to reassess the matter of censorship all over again? To us, there is no need imposed for deconstructing basic concepts pivoting around the phenomenon of Internet censorship; what might be required is those concepts to be replaced in their current social context and present facts. What has to be reassessed is a two-drifted matter; first of all, as ONI experts argue, there should be a reformation of filtering attempts, in terms of transparency, accountability, and inclusiveness, which could be both desirable and beneficial. Secondly, though, in our view, that there should be a revaluation of public perception of Internet censorship and public reaction towards it; there should be a reassessment in what Seltzer calls "Internet Politics".

A methodological-based approach should chime in with a values-based perspective, which deals with issues of civil liberties and rights. Legitimacy of filtering "in any particular context requires close examination by reference to issues of transparency, responsibility and accountability [McIntyre and Scott, 2008] and any filtering regime should embrace those cardinal principles along with the imperative need for inclusiveness.

Accountability is indispensable as it "creates a feedback system where filtering decisions can be challenged and where actors, such as government agencies, must justify and defend their actions or failures to act" [Bambauer, Palfrey, Zittrain, 2004]. Public accountability though depends on transparency; "knowing what is being filtered, by whom, with what purpose and to what extent" [Dutton, Dopatka, Hills, Law and Nash, 2010]. Transparency "requires defining clearly and narrowly the content that is blocked or prohibited; this informs content providers of what material is not permitted and helps citizens understand the values that filtering seeks to implement" [Bambauer, Palfrey, Zittrain, 2004]. Last, but not least comes inclusiveness; according to it citizens should be involved in decision making about filtering appropriate material and certain balance of control between public and private actors should be preserved [Bambauer, Palfrey, Zittrain, 2004].

Even if principles of transparency and accountability are taken under critical consideration, the part of inclusiveness and responsibility that brings mainstream users in the foreground still remains and underlines the lack of political engagement to the proceedings taking place on the Internet. Acting in concert is crucially needed for users in such a participatory medium as Internet. Paraphrasing

Balkin's words, we would say that people lack a vested interest in each other<sup>21</sup>, that they should re-establish.

Apart from censorship practices that turn upon civil rights in general, paternalistic intentions of one state or welfare and protection of the people are listed as further reasons for the support of restrictions. What lies at the heart of these arguments though, argues Hosp, is actually mistrust. People, the argument goes on, believe that the others are more influenced by "bad"<sup>22</sup> information than they are [Hosp, 2004]. Entrusting Internet decisions on the dissemination of ideas to a market dominated by a few powerful state regulators, drives away people, who may have otherwise been trying to "engage in political debate with those ideas, to canvass online opinion, or to view and create art" [Seltzer, 2008]. Decisions regarding, for instance, "what speech is allowed – and what speech is censored – should not be committed solely to the dictates of the dominant private entities that control expression on the Internet" [Nunziato, 2009]. In Seltzer's remarkable words, "reasonable opinions may differ on the propriety of Internet content control, [...] but the Internet's power for information dissemination should at least illuminate that decision" [Seltzer, 2008]. Political institutions can play an eminent role and checks of the political process are crucial for the free flow and future of the Internet. In the long run, when people have more political participation rights, they learn how to use the means of discussion and information is more valuable so that it helps to "reduce mistrust and dampens the demand for censorship" [Hosp, 2004].

## Conclusion

Internet's basic functionality does not include censorship [Brown, 2008]. It can be designed in whatever we want it to be designed [Balkin, 2009]; and it was designed to allow the efficient transmission of information between networks around the world.

Not realizing what this practically means for every each and one of us who uses the Internet, could possibly mean the exclusion of us in the designing process or even worse the ignorance of such a process actually taking place. If this happens, Internet imperils to lose its most vital part, which is consisted of the various dif-

---

21. See Balkin, 2009, p. 110, as it concerns collateral censorship: "Book publishers have a vested interest in the work of their authors, and newspapers have a vested interest in the work of their journalists. But if A is not affiliated with B, A lacks strong incentives to defend B's speech and every incentive to prevent lawsuits. As a result, to avoid liability, A will tend to censor a lot".

22. On "bad" and harmful, potentially, information, see Bottis M., *Information Law*, 2004, pp. 131-133.

ferent ideas and cultural traits that people from around the world contribute interactively.

Subsequently, rating and filtering systems may affect the cultural diversity of cyberspace [Chalaby, 2000] and can have a drastic impact on mainstream Internet users, who have access to information [Brown, 2008], as well as civil society activists, who make extensive use of the Internet in order to carry out their work [Deibert and Villeneuve, 2005]. In addition “the kinds of individual creativity by the personal computer (PC), including self-expression in the form of the creation of user-generated content, might be thwarted by the presence of a censorship and surveillance regime” [Palfrey, 2007].

But how is it possible for someone to know that something has been censored when he doesn't know that it was there in the first place? Seltzer is among the ones to point out the political concerns that blocking and filtering raises; it can be hard for the public to know – she argues – whom to blame or how to protest search removals [Seltzer, 2008].

Personal responsibility towards the matter of Internet censorship should be reconsidered; we cannot continue claiming that we are unaware of internet censorship; Internet censorship is happening. However, “a wealth of information creates a poverty of attention,” pointed out Herbert Simon out a generation ago, and the wealth of information on the Internet which multiplies at an exponential rate may lead us to new upsetting levels of inertia, when everything will seem to follow the rule: out of sight, out of mind; until at least censorship affects us. For example “when a government blocks a website or deletes a weblog comment it is much less public and people may non notice it unless it directly affects them”[Fish, 2009]. The mainstream users may notice if the state blocks an entire website, as Turkey did on YouTube, but even if they do, “the outrage may be limited as competing services can fill the gap” [Fish, 2009].<sup>23</sup>

It is said, the free and open, truly, “world wide” Web is what we are after [Palfrey, 2010]. So, why shall we let it be a dark place that “cybervigilants” [Cammarano, 2002] patrol day and night, while we play carefree in our Internet yard waiting for them to come to our doorstep? If this is a scenario that we choose,

---

23. Another case that may also apply is that of the user in good faith. When we do have already gained and consolidated the basic principles of free speech and privacy protection, warded by legislative provisions and judicial decisions, it is possible to believe in good faith – while having in the meantime a relatively vague and obscure idea of how internet works – that digital world actually works just like the real world does; therefore, as long as we are constitutionally protected and safe against censorship in the real world we tend to feel safe on the internet as well.

eventually Internet will not be a place that we will like to “live in” as it may “very well lead to the end of the Internet as we know it” [Nunziato, 2009]. Citizens will be cut off from information sources and each other and it is quite possible that “the global network value of the Internet will be reduced significantly” [Brown, 2008].

What needs to be apprehended is that Internet cannot remain an “intellectual playground for ever” [Ebbs, 1994] or a ‘Wild West’, lawless and unregulated territory [Dutton, Dopatka, Hills, Law and Nash, 2010]. What is needed at the moment is what Seltzer calls, “an Internet [that] we have democratically chosen and created” [Seltzer, 2008]. More active participation of users in the decision-making process concerning the use of online filtering systems is mandatory in our commitment to preserve Internet alive while transparency among the other above mentioned mechanisms might enable the public towards that direction.

Human rights activists “strive to achieve a balance between the freedom of expression, including the freedom to send and receive information regardless of frontiers or form of government, and private or societal interests in property, security, health, or morals” [Travis, 2011]. Legislative measures against censorship and collective actions in that direction keep pace with the necessity of individual education, in producing and maintaining a democratic polity that is compatible with the principles of freedom of expression, individual privacy, freedom of speech.

It is an imperative need that we are well-educated, well-informed, and conscious about the current facts regarding the Internet; it is important that we cultivate our moral fibres knowing what is happening, being aware and committed to the society’s causes. Only if we know, we will be able to overcome the indirect, often- invisible, disappearance of public speech from intermediate points in the Internet which mutes the political debate around this censorship and we will be able to unite our pressure to the pressure of human rights activists and non governmental organizations (NGOs), against censorship advocates.

Living in a time of crisis the crisis may well be one of conscious. The less we realize and get the time and information that will help us realize of what is happening on the Internet, the more we get to have an illusion of meaningless choice over our actions on the Internet and the less we get to build up a strong consciousness that will lead us in objecting against those practices, in avoiding manipulation and misleading techniques and in designing an Internet according to what we the users want.

Citizens “who value free expression should call for national debate on [censorship] practices, calling attention to the governments and laws that are the source



of pressure and evaluating the effects against free speech principles" [Seltzer, 2008]. A democratic polity in and outside the Internet barriers is what is needed in order the nature of the Internet to be preserved. As Balkin interestingly puts it:

"The digital age makes increasingly clear that the point of the free speech principle is to promote not merely democracy, but something larger: a democratic culture. What is a democratic culture? It is a culture in which ordinary people can participate, both collectively and individually, in the creation and elaboration of cultural meanings that constitute them as individuals. Participation in culture is important to us as human beings because, in an important sense, we are made out of culture; we draw on culture to be the sort of individuals we are. [...] A democratic culture is not democratic because people get to vote on what culture should be like. It is democratic because people get to participate in the production of culture through mutual communication and mutual influence. Democratic culture invokes a participatory idea of democracy" [Balkin, 2009].

It was only in 1996 that John Perry Barlow declared<sup>24</sup>, with his now famous words, that "not only did [...] nation-states had no right to interfere with any

---

24. Raman Ch., Jit Singh, *The Regulation of the Internet With Relation to Speech and Expression by the Indian State*. Raman, 2007, p. 1 In John Perry Barlow's words: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions. You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions. You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different [...]. We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity [...]"

matter relating to the Internet, [but] they also [...] in fact, could not do so even if they wished" as Internet's "nature" resists regulation [Raman, 2007].

Soon after, in 1997 the United States Supreme Court declared in relation to the case *Reno v. ACLU*<sup>25</sup>, which meant to consist a long lasting compass for Internet in its passage through the rocky patches of our times, that "the Internet in encouraging freedom of expression in a democratic society outweighs any theoretical but unproved benefit of censorship" [Chalaby, 2000].

Today, fourteen years after, these words are much more contemporary than ever before; whenever we encounter Internet censorship we should return to the notion and sense of these words. As it was brilliantly alleged in this notorious case *Reno v. ACLU*:<sup>26</sup>

"Internet is the most participatory form of mass speech yet developed. Its content should remain as diverse as human thought"

## References

Balkin J. (2009), The Future of Free Expression in a Digital Age, *Pepperdine Law Review*, Vol. 36, 101-118. Available at SSRN: <http://ssrn.com/abstract=1335055>.

Bambauer D., Palfrey J., and Zittrain J. (2004), "A Starting Point: Legal Implications of Internet Filtering", a publication of the OpenNet Initiative, available at <http://www.opennetinitiative.org>.

Bambauer D. (2008), *Cybersieves*, *Duke Law Journal*, Vol. 59, 2009, Brooklyn Law School, Legal Studies Paper No. 149, 1-60. Available at SSRN: <http://ssrn.com/abstract=1143582>.

Bambauer D. (2008), *Filtering in Oz: Australia's Foray into Internet Censorship*, Brooklyn Law School, Legal Studies Paper No. 125, 1-30. Available at SSRN: <http://ssrn.com/abstract=1319466>.

Banisar D. (2010), Linking ICTs, the Right to Privacy, Freedom of Expression and Access to Information, *East African Journal of Peace & Human Rights*, Vol. 16, No. 1. Available at SSRN: <http://ssrn.com/abstract=1716969>.

---

25. 117 S. Ct. 2329, 138 L. Ed. 2nd (1997). For an analysis of *Reno* and a commentary on the nature of damage possibly caused by harmful Internet content, see Bottis, M., *Prohibition of Censorship and Protecting minors - Internet control of access to pornographic material*, *Human fights*, 31 (2006), pp. 849-894. In Greek.

26. *Id.*

Bendrath R. and Mueller M. (2010), The End of the Net as We Know it?, Deep Packet Inspection and Internet Governance. Available at SSRN: <http://ssrn.com/abstract=1653259>.

Bottis M., Information Law, Nomiki Vivliothiki, 2004. In Greek.

Brown I. (2010), Beware Self-Regulation, Index on Censorship 2010 39: 98-106, available at <http://ioc.sagepub.com/content/39/1/98>.

Brown I. (2007), Internet Filtering - Be Careful What You Ask for. Freedom and Prejudice: Approaches to Media and Culture, Kirca S., Hanson L., eds., 74-91, Istanbul: Bahcesehir University Press (2008). Available at SSRN: <http://ssrn.com/abstract=1026597>.

Cammarano, P. (2002), Internet and the Censorship: Is it Legal (And Necessary) to Censor the Web? 1-23, Available at SSRN: <http://ssrn.com/abstract=346861> or doi:10.2139/ssrn.346861.

Chalaby J.K., New Media, New Freedoms, New Threats, International Communication Gazette, Vol. 62: 19-29.

Chan M.Th., Governments and the Executive "Internet Kill Switch", IEEE Network, March/April 2011, pp.1-2.

Cheng Gr., Cohen M., Green J., Oliveira C., Stadnyk M.&I. Deyrup, Director, The Harvard Law National Security Research Group, Responses to Questions posed by CNAS or International Law & Internet Freedom, p.p.1-26. Available at <http://www.law.harvard.edu/students/orgs/nsrc/CNAS-Final%20Draft-3.pdf>.

Christof D.H. (2002), Central Points of control and Surveillance on a "decentralized" Net: Internet service providers, and privacy and freedom of speech online, available at <http://www.emeraldinsight.com/1463-6697.htm>.

Crandall J., Zinn D., Byrd M., Barr E. and Rich E., (2007), ConceptDoppler: A Weather Tracker for Internet Censorship, paper presented at 14th ACM Conference on Computer and Communications Security, Oct. 29-Nov. 2, 2007.

Comninos A., Twitter revolutions and cyber crackdowns (subtitled) User-generated content and social networking in the Arab spring and beyond Association for Progressive Communications (APC), 2011. Available at [http://blogue.apc.org/en/system/files/AlexComninos\\_MobileInternet.pdf](http://blogue.apc.org/en/system/files/AlexComninos_MobileInternet.pdf).

Condon St., (2009), Google-backed tool detects Net filtering, blocking, available at [http://news.cnet.com/8301-13578\\_3-10152117-38.html#ixzz1K0ulvOgv](http://news.cnet.com/8301-13578_3-10152117-38.html#ixzz1K0ulvOgv)/accessed 14.03.2011.

Deibert R., Palfrey J., Rohozinski R., Zittrain J., eds., (2010), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, MIT Press.

Deibert R., Palfrey J., Rohozinski R. and Zittrain J., eds., (2008), *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge: MIT Press.

Deibert R. and Rohozinski R. (2010), *Beyond Denial: Introducing Next Generation Information Access Controls*, Chapter 1, 1-11, in Deibert R., Palfrey J., Rohozinski R., Zittrain J., eds., (2010), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, MIT Press.

Deibert R. (2003), *Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace*, *Millennium - Journal of International Studies* 2003 32, 501-530, available at <http://mil.sagepub.com/content/32/3/501>.

Deibert R. and Rohozinski R. (2010), *CyberWars*, *Index on Censorship*, 39, 79-90, available at <http://ioc.sagepub.com/content/39/1/79>.

Deibert, R. & Villeneuve, N. (2005). *Firewalls and Power: An Overview of Global State Censorship of the Internet*. In Klang M. & Murray A. (Eds.), *Human Rights in the Digital Age*, 111-124, London: GlassHouse.

Depken C.A., *The Demand for Censorship*, 1-38. Available at SSRN: <http://ssrn.com/abstract=300859> or doi:10.2139/ssrn.300859.

Deva, S. (2007), *Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?* *George Washington International Law Review*, vol. 39, 255-319, 2007. Available at SSRN: <http://ssrn.com/abstract=964478>.

Deva S. (2008), 'Yahoo! For Good' and the Right to Privacy of Internet Users: A Critique, *Journal of Internet Law*, Vol. 11, No. 9, 3-10. Available at SSRN: <http://ssrn.com/abstract=1165483>.

Dutton W.H., Dopatka, A., Hills M., Law G. and Nash V. (2010), *Freedom of Connection - Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*, Dutton W.H., Dopaka A., Hills M., Law G. and Nash V., *Freedom of Connection – Freedom of Expression*, Paris: UNESCO, 2011, 1-105, Available at SSRN: <http://ssrn.com/abstract=1654464>.

Ebbs J and Rheingold H, (1994), *Censorship on the Information Highway*, *Information Management & Computer Security*, Vol. 2 No. 4, 30-31, MCB University Press Limited, 0968-5227.

Electronic Frontier Foundation, *Sites COICA may take offline and why*, available at <http://www.eff.org/pages/sites-coica-may-take-offline-and-why> / accessed 08.11.2010.

Edwards, L. (2009), *Pornography, Censorship and the Internet*, Law and the Internet, L. Edwards & C. Waelde, eds., Hart Publishing, 2009. Available at SSRN: <http://ssrn.com/abstract=1435093>.

Esbin B. S. (2009), *Net Neutrality: A Further Take on the Debate*, Progress & Freedom Foundation: Progress on Point, Vol. 16, No. 26. Available at SSRN: <http://ssrn.com/abstract=1529090>.

Fish E. (2009), *Is Internet Censorship Compatible with Democracy?: Legal Restrictions of Online Speech in South Korea*, Asia-Pacific Journal on Human Rights and the Law, Forthcoming, 43-96, Available at SSRN: <http://ssrn.com/abstract=1489621>.

Gorman G. (2005), *China-bashing in the internet censorship wars*, Online Information Review, Vol. 29 No. 5, 453-456, Emerald Group Publishing Limited, available at [www.emeraldinsight.com/1468-4527.htm](http://www.emeraldinsight.com/1468-4527.htm).

Hills J. (2006), *What's New? War, censorship and Global Transmission: From the Telegraph to the Internet*, The International Communication Gazette, Sage Publications, London, Thousand Oaks&New Delhi 1748-0485, Vol 68 (3), 195-216.

Hosp G. (2004), *Express Yourself! Political Participation Rights and the Demand for Censorship*, 1-26. Available at SSRN: <http://ssrn.com/abstract=591029> or doi:10.2139/ssrn.591029.

Kreimer S.F. (2006), *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*. University of Pennsylvania Law Review, vol. 155, 1-92, No. 11, U of Penn Law School, Public Law Working Paper No. 06-45. Available at SSRN: <http://ssrn.com/abstract=948226>.

MacKinnon R. (2007), *Flatter world and thicker walls? Blogs, censorship and civic discourse in China*, Springer Science and Business Media, 31-46.

Marsden Chr. T., *Net* (2010), Towards a Co-Regulatory Solution, Bloomsbury Publishing at SSRN: <http://ssrn.com/abstract=1533428>.

Marsden, Chr. T. (2010), *Network Neutrality and Internet Service Provider Liability Regulation: Are the Wise Monkeys of Cyberspace Becoming Stupid?*, Global Policy, vol. 2, No. 1., available at SSRN: <http://ssrn.com/abstract=1622324>.

Maurushat A. (2008), *Anti-Censorship, Benevolent Payloads and Human Rights*, UNSW Law Research Paper No. 2008-60, 1-24. Available at SSRN: <http://ssrn.com/abstract=1402425>.

McIntyre T. J. and Scott, C.D. (2008), *Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility*. Regulating Technologies, Brownsword, R.,

Yeung, K, eds., Oxford, Hart Publishing, 1-15, Available at SSRN: <http://ssrn.com/abstract=1103030>.

Miller Cl. C., (2010), Google Reports on Government Requests and Censorship, The New York Times Bits, available <http://bits.blogs.nytimes.com/2010/09/21/google-reports-on-government-requests-and-censorship/> / accessed 10.04.2011.

Nunziato D. (2008), Net Neutrality, Free Speech, and Democracy in the Internet Age, GWU Law School Public Law Research Paper No. 440, Stanford University Press, Forthcoming; Available at SSRN: <http://ssrn.com/abstract=1266365>.

Nunziato D.C. (2005), The Death of the Public Forum in Cyberspace. Berkley Technology Law Journal, Vol. 20, No. 1115; GWU Law School Public Law & Legal Theory Research Paper No. 326, 1-53. Available at SSRN: <http://ssrn.com/abstract=1003415>.

Palfrey J. G. (2010), Local Nets on a Global Network: Filtering and the Internet Governance Problem. Chapter in The Global Flow of Information, Jack Balkin, ed., Forthcoming, Harvard Public Law Working Paper No. 10-41, 1-16. Available at SSRN: <http://ssrn.com/abstract=1655006>.

Palfrey J. (2007), Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet, chapter 1.5, 69-78.

Palfrey J. (2006-2007), Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet. Global Information Technology Report, World Economic Forum, 69-78. Available at SSRN: <http://ssrn.com/abstract=978507>.

Raman Ch., Jit Singh (2007), The Regulation of the Internet With Relation to Speech and Expression by the Indian State., 1-66 Available at SSRN: <http://ssrn.com/abstract=1237262>.

Segal D. and Swartz, (2010) 09:40 AM, Stop the Internet Blacklist, Huffington Post, Hoffpost Politics, available at [http://www.huffingtonpost.com/david-segal/stop-the-internet-blackli\\_b\\_739836.html](http://www.huffingtonpost.com/david-segal/stop-the-internet-blackli_b_739836.html) / accessed 1.12.2010.

Seltzer W. (2008), The Politics of Internet Control and Delegated Censorship, American Society of International Law, 1-6. Available at SSRN: <http://ssrn.com/abstract=1496056>.

Seltzer W. (2008), The Politics of Internet Control and Delegated Censorship (April 10, 2008). American Society of International Law, Berkman Center Research Publication No. 2008-3, 1-6, Available at SSRN: <http://ssrn.com/abstract=1518951>.

Semitsu, Junichi P., *Burning Cyberbooks in Public Libraries: Internet Filtering Software vs. The First Amendment* (April 30, 2010). *Stanford Law Review*, Vol. 52, No. 509, 2000. Available at SSRN: <http://ssrn.com/abstract=1598496>.

Sidak, J.Gr., (2004), *An Economic Theory of Censorship*, Source: Supreme Court Economic Review, Vol. 11, 81-124, Published by: The University of Chicago Press, available at <http://www.jstor.org/stable/3655326>/accessed: 17/03/2011.

Spang-Hansen H., Stakemann H. (2001), *Filtering and Blocking of Websites Content and Legislation on the Internet - Including the Yahoo Case*. *Kritisk Juss* (Norwegian Law Journal - Critical Law), No. 3-4, 321-328. Available at SSRN: <http://ssrn.com/abstract=1092384>.

Spang-Hansen H., Stakemann H. (2001), *The Earthly Chaos in Websites Question of Jurisdiction and Net-Censorship*. *Kritisk Juss* (Norwegian Law Journal - Critical Law), No. 1-2, 63-67. Available at SSRN: <http://ssrn.com/abstract=1092383>.

Travis H. (2011), *YouTube from Afghanistan to Zimbabwe: Tyrannize Locally, Censor Globally*, Florida International University Legal Studies Research Paper No. 11-10, 1-34. Available at SSRN: <http://ssrn.com/abstract=1809952>.

Villeneuve N. (2008), *Search Monitor: Toward a Measure of Transparency*. Available at SSRN: <http://ssrn.com/abstract=1157373>.

Wimmer K. (2006), *Toward a World of Law: Freedom of Expression*, *Annals of the American Academy of Political and Social Science*, Vol. 603, Law, Society, and Democracy: Comparative Perspectives, Sage Publications, Inc in association with American Academy of Political and Social Science, 202-216.

Yunchao W., (2010), *The Art of Censorship*, *Index on Censorship* 39: 53-57, available at <http://ioc.sagepub.com/content/39/1/53>.

ZDNet, "Time to filter out the Internet effluent", 18 August 2004. Available at <http://news.zdnet.co.uk/leader/0,1000002982,39163885,00.htm> / accessed 15.03.2011.

Zittrain J. and Palfrey J. (2007), *Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet*, Chapter 5, 103-122, in Deibert R., Palfrey J., Rohozinski R. and Zittrain J., eds., (2008), *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge: MIT Press.

Zittrain J., 2002, *Perspective: Can the Internet survive filtering?*. Available at <http://news.cnet.com/2010-1071-945690.html#ixzz1JuWj1fUT>/accessed 12.04.2011.

# Internet child pornography and problems in relation to its criminalization

---

---

Vaiani-Vagia Polyzoidou

---

---

## 1. Introduction

Child pornography has been one of the most controversial topics arising from the use of the Internet in recent years - which has already taken dangerous dimensions and it is continuing to spread very quickly. Thus, by late 1990, international and supranational legislator<sup>1</sup> (UN, Council of Europe and European Union), realizing the urgent need to regulate legally child pornography, established legal instruments designed to prevent and suppress the broader phenomenon of pedophilia and pederasty. The main reason was, of course, the staggering spread of the Internet<sup>2</sup>, through which pornographic material is trafficking extremely easily. Moreover as child pornography belongs to cybercrimes<sup>3</sup>, it has a series of features extremely “fearful” such as: its speed, the convenience of committing, the fact that it does not require specialized knowledge as well as it can take place without offender’s removal from his home e.t.c. and free of charge and last but not least the fact that its investigation is extremely difficult<sup>4</sup>. All the above<sup>5</sup>, in combination with the transnational organized way of the pedophile crime<sup>6</sup>, heightened the need for cooperation between states and recognition of harmonized legislative standards in order to come up against child pornography by taking preventive and repressive measures. Consequently, the phenomenon has been a field of special interest for both national and supranational legislator.

---

1. For a short analysis of supranational and international approaches: Akdeniz Y. (2008), p. 163 – 224 as well as Dimopoulos C. (2006), p. 45 – 146.

2. Ahmed K. in Spinellis D. (2004), pp. 216.

3. Furnell S. (2002), p. 25.

4. Quayle E. and Taylor M. (2002), p. 20 - 21.

5. For the definition and the characteristics of “cybercrime”, Clough J. (2010), Yar M., (2006), Williams M. (2006), Speer D. (2000), p. 259 – 273, Strossen N. (2000), p. 11 – 24, Ulrich S. (2004), p. 16, Aggelis I. (2000), p. 678, Zanni An. (2005), p. 63, Lazos G., “Computers and Crime” (2001), p. 211.

6. Tiefenbrum S. (2006), p. 26.



## 2. National Law

The involvement of information systems in the perpetration of child pornography has created a number of new implications to the crime<sup>1</sup>, as it is clearly reflected in Law 3625/2007 –by which digital child pornography was formalized in the Greek Penal Code. As a consequence, today, in the second paragraph of article 348A<sup>2</sup> we meet the crime of child pornography which is committed through a computer system or Internet –an aggravated offense which is punishable more severely than “conventional” child pornography. In particular, the previous article of Penal Code provides that “Any person who produces, provides, sells or otherwise makes available, distributes, transmits, buys, procures or possesses child pornography, or spreads information about the commission of these offenses through a computer system or using the internet, is punished with imprisonment for at least two years and with a penalty of fifty thousand to three hundred thousand Euro”.

### 2.1. *Necessity of separate criminalization*

The significance of specific standardization of digital child pornography can be explained both at a social and at a legal level. First and foremost, the social phenomenon of child pornography in the digital environment<sup>3</sup> has already been on a disturbingly large scale. For instance,

- the websites which contain child pornography –even with infants- have increased by 345% over the last decade,
- the turnover of internet child pornography is estimated to range from 200,000,000 to 1 billion U.S. dollars per year,
- while in Greece the last 10 years these sites increase by 150% per year<sup>3</sup>.

Furthermore, the importance of specific standardization of digital child pornography in the modern era is obvious after a comparison to the pre-Internet era, when pornographic material was real and corporeal. Moreover, different characteristics are attributed both to the victim and to the perpetrator of child pornography in cyberspace. All the above seem to justify, in legal terms, a separate deal with the phenomenon in an online environment. Furthermore, the specific characteristics of the Internet affect the different criminal behaviours of child pornography and they can –in turn- explain the necessity for separate standardization.

---

1. For Internet Crime and Cybercrime in general, Kaiafa – Gbadi M. (2007), p. 1058, Aggelis I. (2000), p.675.

2. Grabosky P. and Smith R. (1998), p. 119.

3. More Statistics in Kioupis D. (2007), p. 6.

## **2.2. Objective Elements of article 348A' Penal Code**

### **2.2.1. Criminal Behaviours – General review:**

After these necessary introductory observations concerning the social dimension of internet child pornography and the characteristics of pornographic material, we can now review the crime as it described in article 348A' 2<sup>nd</sup> Paragraph PC. The definition of child pornography committed through computer system or on-line is a difficult issue, not only in relation to the identification of digital child pornography (as it is defined in the third paragraph of article 348A PC) but also while trying to delimit the individual punishable behaviours that constitute it. Besides, the difficulty in identifying the various behaviours that the crime can take as well as the need for the greatest protection of children has led the Greek legislator to a comprehensive standardization of the behaviours of child pornography. So, the ten different behaviours of the crime are indicative of legislator's intention to criminalize completely every aspect of the crime. Of course, at the same time, he incorporated the requirements of international and european documents but with one great difference:

compliance with international legal instruments was sometimes greater than the required one and in disregard of the provided possibility to exclude of the criminalization. So, the ten different behaviours of the crime –which have been accrued by the legislator in article 348A Paragraph 2 P. C.- create a fairly wide range of criminality and they are displayed as equivalent, despite the apparently greater demerit of them. Moreover, the Framework Decision 2004/68 of the European Union has classified the crime behaviours in 4 wide categories, indicating thus their different severity. However, the Greek legislator did not make use of this "classification", listing without systematization every possible behaviour of digital child pornography. As a result:

- i) some of the behaviours are included in others and
- ii) there is no grading and, therefore, there is no axiological distinction based on the principle of proportionality as far as the threatened penalties are concerned. So, consequently, the characteristics and different demerit of each act remain to be judged in the context of the proportionate assessment of penalty.

### **2.2.2. Comparison of Criminal Behaviours:**

Moreover, the behaviours of the digital child pornography have some things in common with the behaviours of "ordinary" child pornography: for example, the same linguistic terms such as production, provision, distribution, procurement.

However, the electronic element gives new dimensions to them. In other words, the “ordinary” behaviours of the crime acquire different meaning when it is committed online. Typically, production of pornographic material is, for example the creation of pornographic images by any electronic means, especially considering that nowadays the majority of devices can connect to the Internet. For instance, an act of production pornographic material in tangible objects (eg photographs) differs from a production in digital form (e.g. mapping on a computer screen), both in terms of typology and regarding to the result –in other words the difference lays in the production of the pornographic material and in particular its form and the possibility of its storage and transmission. Likewise, by “making available” we mean the posting and dissemination of pornographic images via any internet technology, from simple e-mail to more qualified systems including but not limited to newsgroups, chat-rooms, peer to peer networks<sup>4</sup>, and so-called BBS (Bulletin Board Systems), ie bulletin systems hosting discussions.

In addition, the accurate characterization of some behaviours is highly controversial. For example, is the downloading of child pornography<sup>5</sup> an act of production since it creates a new material<sup>6</sup> –even if it’s still a copy of the original material?

## ***2.3. The specific problem of possession of digital data***

### **2.3.1. The physical dominating in digital world:**

The possession of electronic data is one of the most interesting issues related to the digital child pornography<sup>7</sup>. Traditionally, the possession of obscene materials was not an offence, although production and distribution was. In number of jurisdictions this was also reflected in child pornography laws that did not extend to possession *per se*. Nonetheless, as we have already seen, the advent of digital technology has transformed the way in which child pornography is produced and distributed, and most jurisdictions have responded with a range of prohibitions against all dealings in child pornography<sup>8</sup>. But, how could we define the term of “possession”?

Firstly, according to the majority of doctrine and case law, possession -in general- is the actual, lasting and not instant physical dominating of a person on something in such a way that it would be easy for him to determine at any time its ex-

---

4. Taddeo M. and Vaccaro A. (2011), p. 105-112.

5. Wortley R. and Smallbone S. (2006), p. 12.

6. Nouskalis G. (2006), p. 908.

7. Kioupis D. (2008), p. 14, Bourmas G. (2009), p. 326.

8. *Supra* note 3, p. 251.

istence<sup>9</sup>. However, the limits of physical dominating in the digital world are fluid due to the structure and functioning of the computer. To deal with this fluidity, we have to fill the concept of possession of digital material with other data. For instance, we could say that not only must the owner of P/C have the potentiality of access to a specific P/C (where the pornographic material is stored) but also he should have real will of dominating this material, as well as, he should have already managed in any way these data –in order to establish the dominating link with the particular data<sup>10</sup>.

### **2.3.2. Possession vs Simple Viewing of child pornography:**

Regarding to the mere viewing, now, it would seem implicit to exclude from criminality the cases of a simple following of web sites with child pornography unless it followed by storage. However, there is a problem when the material is automatically saved from the internet on the computer and especially in cases of simple viewing (accidental or not) of child pornography and the consequent automatic temporary storage in RAM, cache memory or temporary files. In other words, visiting the website automatically creates a temporary storage in these media. What usually happens in these cases, is the loss of data that have been loaded into RAM just by switching off the computer.

### **2.3.3. Automated storage in cache disk or temporary files:**

But we could not declare the same when data are automatically saved in cache disk or temporary files<sup>11</sup> - of course when the user has not been involved previously in their settings in order to avoid storage even for a limited period until they are replaced with new data. The German case law dealt extensively with this problem, while seeking for maintain a certain degree of dependence as far as possession of digital child pornography is regard, using specific standards such as the stability and duration of the storage<sup>12</sup>. However, the insecurity that lurks even in such terms in combination with the nature of possession has led some authors to restrict the term of possession provided that it is related, at least, with an act of collection or storage of the child pornographic material from “the owner”. In other words, the possession of digital material constitutes a condition itself, but the possession of digital pornographic material in terms of penal law should be directly related to an action (such as the collection or storage) or an omission (as when somebody has the knowledge and the potential to delete the temporary

---

9. Manoledakis I. – Bitzilekis N. (2007), Pavlou S. (2006).

10. Mpourmas G. (2009), p. 324.

11. Kahan D. (2009), p. 2211.

12. Bourmas G. (2009), p. 324.

files) that create or maintain this situation<sup>13</sup>. Therefore, we could end up in a punishment of the owner of digital pornographic material not only because of his mere possession but also due to his action or omission.

#### **2.3.4. The necessity of possession' s criminilization - points of view and arguments:**

Notwithstanding the above, the necessity of possession' s criminilization is another debatable question. On the one hand it is argued that the criminalization of possession in digital child pornography is required in order to preserve the legitimacy while on the other hand the criminilization of possession is faced as an inefficient arrangement that eventually leads to over-criminalization.

- According to the first point of view, the widespread use of the Internet and the fact that access in pornographic material became extremely easy justifies totally the criminalization of possession. In fact, this argument is based primarily on the rules of supply and demand of the market<sup>14</sup>. In other words, without demand there is no market, without market there is no offer, without offer there is no production and without production there is no violation of legal property, so we need to criminalize the demand<sup>15</sup>. Thus, the criminalization of possessing child pornography should discourage producers from creating more material, since there will be fewer people willing to risk breaking the law and being caught in possession of such material; so producers will have fewer people to sell their product to<sup>16</sup>.

- However, it is quite difficult to prove whether there is -indeed- causality between possession of child pornography and a forthcoming production of it. Besides, we can get a better grip of this argument if we consider cases of possession virtual child pornography (when it is not participated any minor).

- On the other hand, the supporters of possession' s criminilisation claim that it may initially seems that the owner of child pornography does not do something more harmful in comparison to the producer but the truth is that the more the material is spread, the greater is the psychological trauma of the minor victim. Besides, the danger to other minors who might come into contact with this material through Internet is growing<sup>17</sup>.

---

13. Supra note 22, p. 326.

14. Explanatory Report of the Convention on Cybercrime (ETS No. 185), par. 94 – 98.

15. Neumann U. (2011), p. 201.

16. Ost S. (2009), p. 113, Taylor M. and Quayle E. (2003), p. 161.

17. Ost S. (2002), p. 452.

-Another very significant parameter in this debate is the profit. For instance, anybody who pays in order to gain and consequently to possess sexual child material, actually provides a motivation for its production. But, is just the same for anybody that downloads online pornographic material from free websites?

- Furthermore, while considering the real purpose of the provision, we remark that another reason which leads to the criminalization of simple possession is based on the practical difficulty of proving the majority of criminal behaviours that the article 348A' PC includes<sup>18</sup>. So, the legislator's intention is (for example) the demonstration of market or production of child pornography through its possession.

- Although the practical value of such an arrangement (especially in the context of criminal prosecution<sup>19</sup>) is beyond any controversy, however, important questions are raised. Is it, finally, appropriate to punish something that actually would not constitute an offence in order to achieve the punishment of actual criminality?

- In any case, the key argument in favour of the criminalization of possession is the necessity for stronger legal protection of property at stake. The legislator seems to give a stronger ethical and social demerit in all behaviours relating to child pornography in order to provide greater guarantees not only for the minor victims that are presented in pornographic material but also for the minor user of the Internet<sup>20</sup>.

- On the other hand, the arguments against the criminalization of possession are related to the mere definition of possession and especially to the meaning of electronic child pornography's possession. Thus, the problems of its delimitation, for example in cases of automated storage of hardware in computer, is one of the principal arguments of those who think that criminalizing the mere possession of child pornography is a legislative practice that can lead in excesses. Another related argument is that the mere possession of pornographic material does not cause harm to anybody, in particular when it takes place –objectively– only for owner's personal use (without the purpose of committing other criminal behaviours of digital child pornography).

### **2.3.5. Contemporary legal status for possession of digital child pornography and comparison:**

From the above, it is obvious why among the various criminal behaviours of digital child pornography, our interest is focused on the specific examination of possession. What deserves further to be noted is that the current legal status of

---

18. Akdeniz Y. (1997), p. 1.

19. Kioupis D. (2008), p. 14.

20. Mitchell K., Finkelhor D. and Wolak J. (2003), p. 333.

possession of child pornography in Greece just lists it in the catalogue that concentrates every behaviour of committing it in digital format, in contrast with the international and European legislation which refers to it -either while trying to find the legitimacy of the article or by trying to restrict the criminal offense with an explicit provision of exemptions.

For example, the decision framework 2004/68 of the European Union, already mentioned, provided the possibility of exemption -and therefore not criminalizing- in the case of possession of child pornography by someone for his personal use and with the provision of a valid consent from the child participating in the material; that is why the child should have reached the age of sexual consent. Unfortunately, the previous exemption was not adopted by the Greek legislator. As a result, the possession of any digital child pornographic material is now uncritically criminalized, and any attempt to identify and consequently limit this widespread concept of possession relies exclusively on the interpreter of the law or on the judge. After all, the mere meaning of possession, in terms of child pornography, seems to be ultimately inappropriate on the digital world.

#### ***2.4. Penalty Framework and Justification:***

Last, but not least, the endangered penalty context for digital child pornography is stricter in comparison to the “ordinary” child pornography which is described in the first paragraph of article 348A’ P.C. . In particular, between 2 to 5 years imprisonment in combination with a penalty of 50.000 to 300.000 € while the pornography which is not committed through a computer or Internet is punished with imprisonment from 1 to 5 years in combination with a penalty of 10.000 to 100.000 €. This difference in penal treatment emerges from the greater demerit that digital child pornography represents. To be more precise, in child pornography which takes place through a computer system or through Internet we can see an intense insult of legal rights that are protected in article 348A’ P.C. since the electronic media provide the potentiality of easy, rapid, costless and massive worldwide production and distribution of child pornography to everyone. So, the digital media contribute to the extensive exposure of the victim that is shown in pornographic material. This uncontrolled and repetitive procedure results in the perpetuation of child’s (which is represented in the material) degrading treatment as a means of sexual stimulation. That’s why, the digital child pornography is punished more severely.

### **3. Greek Legislator’s and European Union’s Choices**

To sum up, there are two essential components of determining the Internet child pornography in the Greek Penal Code: on the one hand the problematic defini-

tion of significant issues related to the crime, and on the other hand the intention of Greek legislator to control the phenomenon in a catholic way. Besides, that's why we have one of the most severe punishment for internet child pornography –and child pornography in general- in comparison to other European countries. Of course, we should mention that nowadays we find similar response both in the choices that the European Union adopts since in the recent proposal of March 2010 for the abolition of the Framework Decision 2004/68 E. U.<sup>21</sup> reveals the intention to criminalize further behaviours that constitute child pornography. In particular, European Union's intention is resulting from the unquestioned integration of possession in the list of crimes of child pornography without any specific reservation –as it used to be. What is more, it results from the criminalization of knowingly obtaining access to child pornography by means of information and communication technology in order “to cover cases where viewing child pornography from websites without downloading or storing the images does not amount to “possession of” or “procuring” child pornography “, as it is stated in the explanatory report of the text<sup>22</sup>.

#### 4. Review

Both the national current legal status and the latest european changes show clearly that the legislator's duty is his careful balance of interests within a society and their proper serving. Although proved the increased danger of Internet child pornography it should be clear that the “*solution*” through the criminalization must not infringe the principle of using criminal law as ultima ratio<sup>23</sup> and the principle of proportionality. After all, it is interesting to wonder if the punishment of behaviours of Internet child pornography en masse with the same penalty shows probably a “*demonization*” of the phenomenon, as well as if it would be a better punishment of possession of pornographic material only when is accompanied by an intention to traffick it.

---

21. Proposal for a Directive of the european parliament and of the council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, <http://register.consilium.europa.eu/pdf/en/10/st17/st17583.en10.pdf>.

22. Explanatory Report on Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA.

23. Kaiafa – Gbadi M. (2011), pp. 81 – 82.



## References

- Aggelis I. (2000), "Internet and Penal Law" in Penal Chronicles N/2000, pp. 675 – 686 (in Greek)
- Akdeniz Y. (2008), "Internet Child Pornography and the Law": National and International Responses, Ashgate
- Akdeniz Y. (1997), "The Regulation of Pornography and Child Pornography on the Internet" in Law and Technology 1997, p. 1
- Bottis M., "The prohibition of censorship and the protection of minors - control of internet access and Pornographic material", Human Rights, 2006, 31, 847-895 (in Greek)
- Convention on Cybercrime, Budapest, 23.XI.2001, online at: <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>, accessed 18/04/2011
- Council Framework 2004/68/JHA of 22 December 2003 in EE L 13/20.1.2004, online at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:013:0044:0048:EN:PDF>, accessed 18/04/2011
- Dimopoulos C. (2006), "Crimes of children's sexual exploitation, Trafficking, Pornography Carnal Abuse", Nomiki Vivliothiki (in Greek)
- Explanatory Report of the Convention on Cybercrime (ETS No. 185), par. 94 – 98, online at: <http://conventions.coe.int/treaty/en/reports/html/185.htm>, accessed 18/04/2011
- Explanatory Report on Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, on line at <http://www.europeanlawmonitor.org/legislation/2010/COM201094text.pdf>, accessed at 19.04.2011
- Furnell S. (2002), "Cybercrime – Destroying the Information Society" (in Greek)
- Grabosky P. and Russel S. (1998), "Crime in the digital age"
- Jewkes Y. (2002), "Dot.cons Crime, deviance and identity on the Internet"
- Kahan D. (2009), "Child pornography, the internet, and the challenge of updating statutory terms", 122 Harvard Law Review, p. 2206
- Khaled A. (2004), "Who does what to children, where, why and how?" in Greek National Section of the International Association of Penal Law, Dionysios Spinelis (ed.), "Computer Crimes, Cyber-Terrorism, Child Pornography and Financial Crimes", p. 214 e.t.c.

- Kaiafa – Gbadi M. (2011), “European Criminal Law and Treaty of Lisbon” ) in greek)
- Kaiafa – Gbadi M. (2007), “Criminal Law and Abuse of Computer Science” in Armenopoulos 2007: 7, p. 1058 – 1087 (in Greek)
- Kioupis D. (2008), “Child Pornography; Interpretative approaches to article 348A’ PC” in Criminal Word 2008, p. 5 - 19 (in Greek)
- Kioupis D. (Marangopoulos Foundation for Human Rights) (2007), “Internet Child Pornography” (in Greek)
- Lazos G. (2001), “Computers and Crime” (in Greek)
- Manoledakis I. – Mpitzeleki N. (2007), “Crimes against property” (in Greek)
- Mitchell K., Finkelhor D., Wolak J. (2003), “The exposure of youth to unwanted sexual material on the Internet: a national survey of Risk, Impact and Prevention” in Youth and Society, Vol. 34 No. 3, March 2003, p. 330 – 358
- Mpourmas G. (2009), “Conceptual efforts of identifying the possession of electronic data in child pornography” in Criminal Justice 3/2009, p. 322-327 (in Greek)
- Neuman U. (2011), “The criminal responsibility of the market participants - on the spread of the Criminal Law in precautionary Criminal Law” in Kaiafa Gbadi M. and Prittwitz C., (eds.) “Surveillance and law enforcement in contemporary criminal policy”, p. 199
- Nouskalis G., (2006) “Child Pornography: The crucial issues of article 348A’ PC” in Criminal Justice 7/2006, p. 908- 915 (in Greek)
- Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography of 25 May (2000) 2000, A/RES/54/263, online at: <http://www2.ohchr.org/english/law/crc-sale.htm>, accessed 18/04/2011
- Ost S. (2009), “Child Pornography and Sexual Grooming- Legal and Societal Responses”, Cambridge University Press
- Ost S. (2002), “Children at risk: Legal and societal perceptions of the potential threat that the possession of child pornography poses to society” in Journal of Law and Society, Volume 29, Number 3, September 2002, pp. 436- 460
- Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, website: <http://www.europeanlaw-monitor.org/Current-Directives/EU-Directives-2010/COM-2010-94-Proposal-for-a-DIRECTIVE-OF-THE-EUROPEAN-PARLIAMENT-AND-OF-THE-COUNCIL-on-combating-the-sexual-abuse-sexual-exploitation-of-children-and-child-por>

nography-repealing-Framework-Decision-2004/68/JHA.html and <http://register.consilium.europa.eu/pdf/en/10/st17/st17583.en10.pdf>, accessed 10/8/2011

Pavlou S. (2006), "Crimes against property" P.N. Sakkoulas, (in Greek)

Sarzana C. (2003), "Informatica, internet e diritto penale" (in Italian)

Sieber U. (2004), "Computer Crimes, Cyber-Terrorism, Child Pornography and Financial Crimes (General Report)" in Greek National Section of the International Association of Penal Law, D. Spinellis (ed.) "Computer Crimes, Cyber-Terrorism, Child Pornography and Financial Crimes", p. 16

Speer D. (2000), "Redefining borders: The challenges of Cybercrime" in *Crime, Law and Social Change*, 34, pp. 259 – 273

Strossen N. (2000), "Cybercrimes vs Cyberliberties" *International Review of Law, Computers and Technology* 14, pp. 11 – 24

Symeonidou – Kastanidou E. (2006), "Crimes vs Personal Interests", *Nomiki Vivliothiki*, (in Greek)

Symeonidou – Kastanidou E. (2003), "Human trafficking in the international environment and Greek law's criminal response" in Symeonidou – Kastanidou E. "The new law 3064/2002 on human trafficking", p. 15 – 50 (in Greek)

Taddeo M. and Vaccaro A. (2011), "Analyzing Peer to Peer Using Information Ethics" in *The Information Society*, 27:2, pp. 105-112

Taylor M. and Quale E. (2003), "Child Pornography: An Internet Crime" Routledge

Tiefenbrum S., (2006) "Child Soldiers, Slavery, and the trafficking of children", online at: [http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=susan\\_tiefenbrun](http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=susan_tiefenbrun), accessed 18/04/2011

Theodoridis K. (2007), "Internet Child Pornography" in *Revue hellénique de droit européen*, 3: 2007, p. 671 – 680 (in Greek)

Quayle E. and Taylor M. (2002), "Child pornography and the Internet: Perpetuating a cycle of abuse", *Deviant Behaviour* 2002, 23 (4), pp. 331 - 362

Wall D. (ed.) (2003), "Cyberspace Crime", Aldershot

Zanni A., (2005) "The Cybercrime", Sakkoulas A. (in Greek)

# **“Illegally obtained evidence and their use in civil procedure”**

---

---

**Ioannis Revolidis**

---

---

## **I. Generalities**

“A theologian asked an almighty computer if there’s a God. The computer answered that it didn’t have the necessary processing capacity to know. He asked to have it connected to all other supercomputers of the world. But still it was not powerful enough. So, they connected the computer to all host computers, microcomputers and personal computers. Finally, it managed to connect to car computers, microwaves, digital clocks etc. The theologian asked for the last time if there’s a God. The computer answered: Now there is!”. The semiotics of this story originating from the mid 90’s, can be found in fears as well as in expectations arisen worldwide from the explosive rise and wide spread of electronic networks. Many of the expectations of that time have been fulfilled, yet many of the fears as well were proven to be true, which today are even some of the most important challenges for the Law and not only.

In the early 70’s, when the modern world entered the third phase of the industrial revolution, in which the digitalization of information data started rising gradually, mainly concerning activities involved in administrative or military organization of most societies but also concerning scientific research, no one could have predicted that modern social aggregations would increasingly depend on electronic communication networks. This event was roughly called “digital industrial revolution” and its growth during the years that followed, posed new social issues and new social challenges. The personal computer was no longer only part of the user’s little world at his office, nor part only of the limited local network of a business or research team. It became by then a means to enter the global information highway of internet.

Internet fulfilled and implemented at a great extent the basic demand of the western societies (mainly after 1989 and after the collapse of the actually existing socialism) for the transition to an increasing globalized traffic of goods and delivery of services. The ability for people to enter the cyberspace from any continent of the planet, as well as the establishment of transaction contacts where the physical presence of their subjects was not any longer requested has profoundly changed the traditional value framework of the markets. Like any revolution, the

digital revolution was accompanied by far reaching reforms in everyday life. The new-fashioned information society is now an international social forum. In this new globalized framework the privacy of individuals became vulnerable in many ways. Without realizing it in its full extent, individuals leave nowadays their digital traces during any kind of their actions, often exposing their private life to an extremely broadened social space. This issue couldn't be of no consequences on the regulatory action of most societies in which it occurred.

The issue of legal regulation of information society has been raised by realizing almost at the same time the wide spread of information. Law reacted rather instinctively and confused. The particularity of information society and especially (in relation to the traditional social phenomena) the different manifestation of most of its aspects (such as the ability to incorporate new and continuously developing technology as well as the ability for individuals from different social groups to participate in it), has triggered a new, for the legal system, kind of discussion regarding its regulation. The standpoints covered the entire range of spectrum beginning from one end, namely considering the information society as a space outside the law regulating by itself any arising conflicts, and reaching the other end, namely the suffocating supervision and strict control of information society by the respective legal order in which it was manifested. In-between standpoints considered that the particularities of information society do not reach the point of disputing the value and usability of the traditional legal framework, which with the necessary interpretive adjustments, could be applied on the information society as well.

In respect of the character that should be assigned to the regulation of information society by the law, the above standpoints soon moved on to the civil procedure level (in Europe as well as internationally), where the conflict of fundamental rights and questioning of traditional legal values began to show within the question of illegally obtained evidence. In fact, the question raised on that level was more serious since the conflict of fundamental rights did not exist as an abstracto discussion but as an in concreto problem of the entire system of the administration of justice.

Now, how should procedural legal order react when the only evidence introduced to a civil court, is obtained illegally and especially through invasion of the individual's privacy by the parties through the internet? Following must preliminary be noted: a) the above problem does not have the same gravity when the illegally obtained evidence is not the only available evidence but is part of a number of evidence introduced by the parties. The judge can then legally base its conclusion on the remaining evidence, even if the judge practically did take into consideration the illegally obtained evidence and b) theories that consider information

society as a space functioning outside the law could not be taken into consideration, since it is not certain that they could provide solutions to the problem in question.

## II. The arising problem

As mentioned above, the science of civil procedural law has already faced in the past the problem of illegally obtained evidence. This rather old question gets new dimensions in the information society. The particularity of the digital environment of internet as well as its global range penetration has intensified the concern on the protection of privacy, given the fact that it was now easier than ever to obtain personal data from one of the parties. Email services, social networking sites, E-market web-pages, electronic forums and blogs are only some of the digital spaces visited by millions of users every day. At each visit the users leave digital traces and data of personal nature that compose together their personality. The creation of "digital profiles" is therefore quite often, based on websites visited by an internet user. The easy way by which an individual can be identified (e.g. through the IP address of its personal computer or its email), as well as the relevant ability to supervise the visited websites, verify without much of a doubt, how easy it is today to intrude the privacy of the subjects in information society. This penetration and gathering of personal data resulted thereby, is being used not only for private or commercial purposes but today also for purposes of a civil court, since often one of the opposite parties manages to detach private information of the other party, which could be decisive for the procedure outcome.

The following cases, which reached the Greek Courts, demonstrate the real dimension of the problem. The facts of the cases have been simplified in order not to put into question the breach of the parties' personal data:

First example: In order for A, husband of B, to support a legal action filed against her in order to obtain dissolution of their marriage by exclusive liability of the wife, he introduced at the hearing and submitted at the court electronic letters sent and received from the electronic mail address of his wife. According to the opinion of the plaintiff A, the content of those letters was erotic and proved that his wife had an affair with another man. It is noted that A did not obtain any consent from his wife B to access her email account, nor did he obtain her consent to detach these particular letters. At the same time, this specific email account belonged exclusively to his wife and was not a common use account.

Second example: The second case deals with posting of personal information of one of the parties on a social networking site by the other party. In particular, A was a teacher at the department of journalism and mass media of a university and at the same time candidate for a position in the scientific teaching personnel as a

assistant professor or associate professor in the cognitive field “Journalism: social and cultural coverage” announced at the same institution. The position in question was initially announced at the end of 2005, so A had submitted a complete candidacy file containing all documents related to her academic, journalistic and professional career. Finally, the procedure ended with no result and the position was announced at new in 2008. While the new announcement was still pending, in October 19<sup>th</sup> 2008 various texts were posted on the website “facebook.com” on a special area created by an unknown user with the alias-name “P.P” und under the title “H.P. and all the friends”. In these texts the unknown author used insulting comments on A, questioned her degree titles (master and doctor degree) and claimed that she was acting under the orders and was close friend of an assistant professor of the department, who would illegally promote her to receive the announced position (as claimed by the unknown author).

Further on new slanderous texts on A were posted, sent also as electronic messages to a list of approximately three hundred (300) electronic addresses of individuals who were academics, politicians and journalists. B was an assistant professor at another educational institution and co-candidate of A for the above mentioned position. On November 10<sup>th</sup> 2008 he submitted to the secretary office of the department of journalism at the aforementioned institution a request and by claiming a number of publications on the internet “with complaints against his opposing candidate (namely A) for the position of the associate – assistant professor, he asked to receive as soon as possible copies of 1. all her study degrees submitted to the secretary of the department, 2. all certificates issued by the Hellenic National Academic Recognition and Information Center concerning the recognition of those degrees, 3. all certificates of her vocational occupation, 4. her doctoral degree, 5. her teaching notes and 6. the text of her lecture at Harvard University. In order to obtain the copies, he claimed legal interest in his capacity as a co-candidate of applicant A for the announced position.

At the end of his application he noted: “If my co-candidate requests a copy of any of the documented contained in my candidacy file, please provide it to her without any delay and as soon as possible as stipulated by law”. On the same day by submitting another request to the Rector of the educational institute, he protested because the head of the secretary office of the department of journalism refused to furnish the requested documents, claiming that he should prior speak on the telephone to the vice-chairman or the chairman of the department, which was impossible to take place on that day. He also spoke about an intentional and illegal “manipulation”. When A learned about the request of B, she decided to give him herself the requested documents. Therefore, she asked a final-year student to deliver a batch of documents to an employee of the secretary office and this employee should further on deliver the documents to B by signing a delivery

receipt of the documents. Prior to the delivery of the documents to B, a delivery receipt was drawn up stating in a list the delivering documents. All the above documents were in the file of the supporting documents submitted by the candidate in 2005 for her candidacy on the announced position, except for some other documents which A copied from her personal file. As soon as the list was drawn up, B came to the secretary office of the educational institution. The employee handed out the documents in a closed envelope and asked B to sign the delivery receipt with the list of the delivering documents. Although B received the envelope, he refused to sign and left. He claimed that the employee handed out to him a closed envelope saying that A sends it and that this envelope contains only some of the documents he requested.

However, it was proven that the envelope did contain all these documents and that B refused to sign the delivery receipt and left. It was also proven that on the same day the pre-mentioned webpage hosted information that was not contained in the file of the year 2005, but only in a document that was delivered to B by A from her personal file. On a following day, documents that were included in the file of 2005 delivered by A to B were posted on the internet. Together with those documents, the documents that were not contained, as already mentioned, in the candidacy file of 2005 but were delivered to B by A, were also posted on the internet. Later on nine (9) more documents from the file of 2005 were posted, while a bulk email to the aforementioned group of the three hundred (300) recipients sent by the unknown P.P, contained letters of reference delivered by A to B.

At the end, the same webpage hosted the university notes of A, which were never published nor were ever distributed to students. In fact, they were contained only in her file and in a copy in the candidacy file of 2005. Please note, that no one else expressed any interest in obtaining copies of the pre-mentioned documents. So the only one that could have them was B. It was proven that he did post all the documents concerning the employment conditions and the professional career of A, without her consent. A delivered B the documents only as an information since he was her co-candidate. In fact these postings on the specific webpage, where anyone could have access to (especially by the search machine where the user could write the name of A and be led automatically to this webpage), were at the same time a violation of A's privacy, since there were accompanied by inappropriate and demeaning sentences (e.g. here are the Greek references on our A") and gave the impression that they were proof of the fact that the degrees of A were illegal but also that she had connections to politicians who were helping her. Of course B claimed not to have the required technical knowledge to be able to do on his own the above actions, but the Court was convinced that the postings was an act of A himself by using a person with the necessary technical knowledge. B, though he received the document file only for his personal use, he



showed them at least to the witness who testified at the court hearing on his initiative (legal right of B).

In the above example cases, one of the parties violated through the internet, the personal data of the other party and obtained in this way evidence. The question raised, focuses on whether illegally obtained evidence implies procedural inadmissibility in a civil court.

### III. Suggested solutions

The question whether substantial illegality could be transformed into procedural inadmissibility, when one of the parties violates the privacy of the other party through the internet is not addressed always in the same way. In the entire discussion, the different approach of the various legal orders in relation to the regulation of information society plays a key role. As long as a legal order considers information society to be a space that cannot be regulated by law, it hopes to deal with this problem by relaying on reflexes and self-regulation procedures that could appear inside the information society itself. Other legal orders, on the other hand, choose to regulate by legislative instruments, issues regarding protection of the privacy of the subjects of information society, by taking special measures also for the transformation of the substantial illegality into procedural inadmissibility.

The issue of illegally obtained evidence is an old concern of the Greek civil procedural law. Within the relative question, all possible aspects were supported: a) illegally obtained evidence is not procedurally inadmissible, given that the substantial illegality cannot be transferred to the procedural level. Besides, according to this aspect, in the civil procedure the most important thing is the correct administration of justice, therefore in order to achieve this goal, illegally obtained evidence could be used as well, and b) the illegal character of obtaining evidence, specifies also its procedural use as inadmissible, given that the legal order is consistent, while it was claimed with convincing argumentation that the elevation of the substantial illegality into procedural inadmissibility could not be based only on the issue of the legal order's consistence, but on the aspect that the system itself of the Greek code of civil procedure provided sufficient entitlement.

The establishment of information society, as mentioned extensively, created new challenges and set the discussion on a new basis. These new challenges contributed to the realization of the newly arisen need to create new rights which could apply in the civil procedure as well. In 2001, the legislator in revising the Constitution, took into consideration the new arisen needs and adopted significant substantial rights and procedural prohibitions, putting finally an end to the discussion on illegally obtained evidence. It is worth noticing, that despite the fact that the new rights could be concluded from already existing regulations of the

Greek Constitution, the legislator preferred to explicitly establish the rights, so that especially the Greek legal order can adjust to the continuously changing and in all times unforeseen challenges arisen by the participation of individuals in the information society. The establishment of the new rights was not only a confirmation but prevention as well. In virtue of the new clause 9A and the two new sub-clauses added to clause 19, the Greek constitution explicitly guarantees the protection of personal data against collection, processing and use through electronic means, as well as through non-electronic means. At the same time it clearly forbids, before any court (civil, criminal, administrative) or instrument and in any procedure, the use, by any means, of evidence obtained by illegal processing of personal data or by violating the confidentiality of responses. The constitutional legislator has established the fact that the protection of personal data as well as the protection of the confidentiality of responses would be rather worthless if not accompanied by its corresponding procedural dimension. The protection would not be complete if the illegally obtained material could be used without any hindrance before civil courts (and before any other court).

The right of informational privacy established by clause 9A of the Constitution, is thusly procedurally secured by the regulation of clause 19 § 3. The constitutional prohibition to use illegally obtained evidence in a civil court by virtue of clauses 9A and 19 § 3, corresponds legislatively and meets the conditions for its consistent practical appliance, to the provisions of law 2472/1997, by which Greece has incorporated into its domestic law the Directive 95/46 EC of the European Parliament and Council regarding the protection of individuals against processing of personal data and the free circulation of this data. Only then is allowed to use evidence obtained by collecting and using personal data, when the collection and use do not constitute a breach of clauses 4, 5, 7 and 7A of law 2472/1997, regulating the conditions of legitimate processing of personal data. Therefore, when a data is subject to the appliance field of law 2472/1997 and hence is a personal data (for non personal data, the evidence prohibition may result from other constitutional provisions protecting the fundamental rights or from provisions of the civil procedure code, the question if it can be used before a civil court can be answered under following regulatory condition: if it is a "simple" personal data, the carrier of the personal data can consent to its collection and processing.

On this particular category of personal data, as an exemption the collection and processing is allowed even without the consent of the carrier, provided that the, in law 2472/1997 restrictively documented exemptions are concurrent. For example, under clause 5 sub-clause 2, section e' of law 2472/1997, the processing of the subject's data without consent, when it is absolutely necessary in order to satisfy the legal interest endeavored by the responsible person for the processing or the third party or parties to whom the data is announced and under the

self-evident condition that the need for processing has more gravity in relation to the rights and fundamental constitutional freedoms of the individuals being processed. In short, the exceptional processing of personal data of an individual without its consent for the satisfaction of the legal interest of the responsible person for the processing, can take place only if it is absolutely necessary and obviously more important than the interests and fundamental freedoms of the processed subject. As to the “sensitive” personal data (clause 7 law 2472/1997), on the contrary, the legislator’s regulation is indeed more strict. In this case, the collection and processing of data is forbidden and is tolerated only by exemption, upon relative permission given by the Hellenic Data Protection Authority and provided that the terms of § 2 clause 7, law 2472/1997 apply. However, the above protective framework becomes relative through the regulation of clause 7A law 2472/1997, which allows the processing of “sensitive” personal data without the permission given by the Hellenic Data Protection Authority when one of the cases documented in its second sub-clause is concurrent.

For the problem under discussion it is very interesting to mention the regulation of clause 7 § 2 section. γ of law 2472/1997, which foresees following: “... Exceptionally, the collection and processing of personal data is allowed when ...: c) the processing relates to data published by the subject itself or when the processing is necessary in order to acknowledge, exercise or defend a right before a court or a disciplinary instrument ...”. Under to the dominating opinion, this provision applies also on the simple personal data, in virtue of the interpretive principle from major to minor, with the particularity that in the case of “simple” personal data, it is not necessary to obtain a permission by the Hellenic Data Protection Authority for processing data. The importance of the regulation for the field of civil court is significant, since the legislator attempts in this way to combine the conflict of the parties’ fundamental right of evidence with the compelling need to protect the privacy of individuals. Even if the processing of simple or sensitive personal data is allowed without the subject’s consent in order for the responsible person of the data processing to defend its right before a civil court, the processing is still subject to the limitation of the purpose and necessity: it shall be allowed to process data only to the extent needed to fulfill the purpose of defending a right before a civil court. Any processing exceeding this limit shall be automatically considered as illegal and thusly leads immediately to an procedurally inadmissible evidence

The, in advance, limited territorial range of a spatially finite legal order, however, cannot cover the needs of privacy protection in the modern globalized framework of information society. The European Union, by realizing relatively soon this problem, took action in order to uniform the level of privacy protection on a community level, in an attempt to exceed beyond any spatial limits set by the

classical private international law. The result of this attempt was the fundamental Directive 95/46 EC of the European Parliament and Council regarding the protection of individuals against processing of personal data and the free circulation of this data. This Directive, despite the compelling need for its modernization and adjustment to the new technology data, remains a basic flag of the community law in terms of privacy protection. In information society, the protection of privacy is completed by the directives 2002/58/EC and 2006/24/EC. At this point we must also mention the significant contribution of the Lisbon Convention in the attempt to secure private life from external (electronic or non-electronic) violations. By clause 6 of the Convention, the Map of Fundamental Rights of the European Union has a binding effect for the state members. Clauses 2, 7 and 8 of the Map of fundamental Rights establish the protection of the human value as well as the protection of the individual's private and family life, while the protection of personal data from external violations is also explicitly established.

The contribution of the Court of the European Community (already Court of the European Union) has been very important in terms of securing private life from violations taken place in information society. In virtue of the fundamental resolution *Bodil Lindqvist* (case C – 101/2001), the Court ruled already at the beginning of the past decade, that the posting of personal data on the internet is an illegal processing of personal data. Moreover, the Court of the European Union in cases C – 275/06 (*Productores de Musica de Espana (Promusicae) vs Telefonica de Espana SAU*) and C – 554/07 (*LSG – Gesellschaft von Leistungsschutzrechtern vs Tele2*) applied the above mentioned case law in matters of procedural character, highlighting, thus, that the protection of individuality provided by Directives 95/46, 2002/58 and 2006/24 is not neutralized in the field of civil procedural law. In the light of the above regulatory provisions and the currently valid decisional law of the Court of the European Union, we would dare to say that the fundament for the dogmatically smooth transition from the substantial illegality to the procedural inadmissibility has been set.

The key importance contributed to the protection of privacy as well as the increased level of protection set by the existing community institutional framework, would justify rather a dogmatic attempt in the direction to an (at least) interpretative modernization of the legal categories “substantial illegality” and “procedural inadmissibility”. The protection of privacy in information society would not seem to be complete if it has no procedural correspondence. The unconditional violation of personal data during a court proceeding would leave a wide field of breaching the community law regarding the protection of privacy and would drastically harm its effectiveness. The unification of the level of the protection of personal data in Europe must inevitably pass through the procedural path.

Though the European institutional framework provides more or less sufficient entitlement for the protection of personal data on the level of substantial law and procedural law as well, the question if this applies also globally, remains unanswered. Like most of the national legal orders, the European legal order as well sets specific spatial boundaries, which drastically limit the effect of the community legislative instruments. The appliance of Directive 95/46/EC cannot stand outside the European Economic Area. The globalized dimension of information society often poses the question of processing personal data of individuals residing in Europe, by persons responsible for data processing established in other geographic continents. Besides, equally often, the level of personal data protection in countries where the processing takes place is not proportional to the one encountered in the European Union. The means of classical private international law seem not to provide satisfactory solutions when seeking an international jurisdiction of the legal order which shall rule on the cases of personal data processing: every time the means of classical private international law shall result in affirmation of international jurisdiction of a legal order where the level of the protection of privacy is weak, the legislative armory of legal orders which took measures for its substantial and procedural protection shall lose its meaning. The achievement of the goal to protect individuals being violated by third parties in their private life, a goal set by most of the legal orders of the western world, presupposes the interpretive transformation of traditional value constants of the private international law (at least as long as the international cooperation and the effort to create a common international protection framework do not result in practically useful outcomes), in a direction that leads to a best possible protection of privacy. The more substantial and procedural guarantees a legal order offers, the more the interpreter and applier of law should ensure to choose it in order to decide on a personal data processing case. The judgment on international jurisdiction, as already ruled by a explicit legislative intervention for other cases of preventive substantial regulation (see clauses 8 f., 15 f., and 18 f. EC 44/2001), must be led by the increasing need to protect the human value and personal data.

#### **IV. Instead of an epilogue**

The value of the human personality and privacy of individuals, a domain of the liberal social revolutions that took place in the past centuries, is unrestrained put in question by the new challenges of information society. The easy way by which third parties can intrude the privacy of individuals and detach any kind of personal information, makes privacy of subjects in an information society vulnerable in many ways, while self-regulating reflexes of information society seem not to be evolved to the extent needed to ensure a substantially and procedurally complete and critical protection of personal data. Illegally obtained evidence regarding the

privacy of one of the parties and the use of it, has a new globalized dynamics. The overall awareness and legal regulation of such dynamics cannot take place within an environment of national or regional isolation. The classical dogmatic constants of private international law, but also the fundamental right of evidence are put in question by the existential conflict with the increasing need to protect privacy. The interpretive release of the intensity and conflict field of those rights in the light of technology in information society, is a challenge that belongs to the future.

## References

Alivizatos N. (2001), Privacy and transparency: A difficult conciliation, L. Sicilianos & M. Gavouneli (eds), Scientific and Technological Developments and Human Rights, Ant. Sakkoulas p. 117 (In Greek).

Allen A. (1988), Uneasy access, Privacy for women in a free society, To towa, N.J.: Rowman & Littlefield, 1988 (In Greek).

Anthopoulos H. (1993), The problem of functional commitment to fundamental rights. (In Greek).

Benabou Valerie – Laure (2001), Should there be a minimum harmonization of the law?, online at <http://droit-internet-2001.univ-paris1.fr/ve/page004.html> \ accessed 22.03.2011. (In Greek).

Benn St. (1971), Privacy, Freedom, and Respect for Persons. (In Greek).

Beys E. (2001), Admissibility invoked recording private conversations conducted without the consent of the participant, Diki, 32, 519. (In Greek).

Bloustein E. (1964), Privacy as an Aspect of Human Dignity: An answer to Dean Prosser, N.Y.U.L Rev., 39, 962.

Brandenburg C. (2008), The newest Way to Screen Job Applicants: A social Networker's Nightmare, Fed. Comm. L. J., 60, 597.

Cheh M. (2001), Technology and privacy: Creating the conditions for preserving Personal Privacy, in Scientific and Technological Developments and Humans Rights, Sicilianos, L.A. and Gavouneli, M. Eds, Ant. Sakkoulas, Athens, p. 99.

Choo Andrew L – T. (1989), Improperly obtained evidence: a reconsideration, Legal Studies, 9, 261.

Chrysogonos K. (2006), Individual and Social Rights. Benabou Valerie – Laure (2001), Should there be a minimum harmonization of the law?, online at <http://droit-internet-2001.univ-paris1.fr/ve/page004.html> \ accessed 22.03.2011. (In Greek).

Dagtoglou P. (1991), Constitutional Law - Individual and Social Rights, A and B. (In Greek).

Dimitropoulos A. (2002), The Constitution as the basis of the legal system. (In Greek).

Donos P./L. Mitrou/Mitletton I./Papakonstantinou Ev. (2002), The Data Protection Authority and the promotion of rights protection. (In Greek).

Fatouros A. (2001), Technological Development, Human Rights and Cultural Diversity, in: Linos Alexandros Sicilianos and Maria Gavouneli (editors), Scientific and Technological Developments and Human Rights, Ant. Sakkoulas, Athens, p. 261.

Gavison R. (1980), Privacy and the Limits of Law, Yale L.J., 89, 421.

Gerontas A. (2002) The protection of citizens from the electronic processing of personal data. (In Greek).

Gesiou - Faltsi N. (1985), Law of Evidence. (In Greek).

Giddens A., (2002) Sociology, Polity Press, 5th. edition.

Giddens Anthony (2001), The consequences of modernism (In Greek).

Guo R. M. (2008), CYBERLAW: Note: Stranger Danger and the Online Social Network, Bekerley Tech. L.J., 23, 617.

Hashemi Y. (2009), Facebook's privacy policy and its third-party partnerships, B.U.J.SCI. & Tech. L., 15, 140.

Iglezakis I. (2003), Sensitive personal data. Sakkoulas Publishers (In Greek).

Iglezakis I. (2004), Publication and transmission of personal data via the Internet, bilateral agreements concluded, 1, 498. (In Greek).

Iglezakis I. (2010), Illegal evidence. Letters via the Internet, bilateral agreements concluded, Dimee 6, 401. (In Greek).

Kaisis A. (1986), Illegally obtained evidence. (In Greek).

Kalavros K. (1991), The tape in civil proceedings. (In Greek).

Kaminis C. (1998), Illegal evidence and constitutional guarantee of individual rights. (In Greek).

Kang J. (1998), Information Privacy in Cyberspace Transactions, Stan. L. Rev., 50, 1193.

Katsh M.E. (1995), Rights, Camera, Action: Cyberspatial settings and the First Amendment, Yale Journal Law, 104, 1690.

Kiki G. (2003), Freedom of the media (in light of the constitutional revision of 2001). (In Greek).

Komnios K. (2010), The legitimacy of web applications-D mapping and virtual tours (Google Street View), DIMEE, 6, 170. (In Greek).

Kousoulis S. (1992). Modern forms of written transactions (Telex - Telefax - Electronic document), Athens-Komotini: Sakkoulas Publishers (In Greek).

Lessig L. (1996), Reading the Constitution in Cyberspace, Emory Law Review, 45, 861.

Lessig L. (1998), Code and other Laws of Cyberspace, Basic Books.

Manesis A. (1982), Constitutional Rights, vol. a, civil liberties. Thessaloniki, Sakkoulas Publishers (In Greek).

Manitakis A. (2001), Constitutional organization of the state, State - Nation - Constitution - Sovereignty - Globalization. (In Greek).

Manoledakis I. (2002), Freedom and Security. Athens-Thessaloniki: Sakkoulas Publishers (In Greek).

Millier S. L. (2009), The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet, K.Y.L.J., 97, 541.

Mitrou L. (2001), The law in the information society. Athens-Thessaloniki: Sakkoulas Publishers (In Greek).

Mitrou L. (2009), Post on facebook documents containing personal data and defamatory comments, DIMEE, 5, 400. (In Greek).

Mitrou L. (2010), The privacy of web 2.0, DIMEE, 6, 319. (In Greek).

Mitsopoulos C. (2002), "Tritenergeia" and "proportionality" as the provisions of the revised Constitution, IDB, p. 641. (In Greek).

Nikas N. (1999), On the admissibility of unfairly acquired evidence, Legal Studies, 251. (In Greek).

Nikas N./Diamantopoulos C. (2004), The potential use in civil proceedings of evidence illegally obtained, Hellenic Justice, 44, 694. (In Greek).

Nikolopoulos G. (2005), The law of evidence. Athens: Ant. Sakkoulas Publishers (In Greek).

Orphanoudakis S. (2003), The principle of proportionality in the Greek legal system. From the case-law application of the constitutional guarantee. (In Greek).



Panagopoulou - Koutnatzi F. (2010), The social networking sites as national, European and International Challenge of Privacy. Ant. Sakkoulas (In Greek).

Paraskevopoulos N. (2002), The law and the challenge of globalization. (In Greek).

Piskopani A - M. (2009), Protecting the privacy of the users of facebook, DIMEE, 5, 338. (In Greek).

Sykes Ch. (1999), The End of Privacy: The Attack on Personal Rights at Home, at work, Online, and in Court, St. Martin's Griffin.

Takis A. (2002), Information Society and Constitution, NoB, 51, 28. (In Greek).

Tsolias C. (2006), Maintaining and processing data in electronic communications in accordance with Directive 2006/24/EC, DIMEE, 3, 347. (In Greek).

Venizelos, Ev. (2002), The Revisionist acquis. The constitutional phenomenon in the 21st century and the contribution of the revision of 2001. (In Greek).

# Advergaming: A lawyer's take

---

---

Veljko Smiljanić

---

---

## 1. Introduction

“Can you pitch a product to a god when even mortals  
go out of their way to avoid us?”

Ilya Vedrashko

Advertising is crucial in the age when information is paramount, and presence on the stage highly coveted. Little space should be devoted to extolling the virtues of new forms of media in getting ideas or products noticed<sup>1</sup>. Advergaming is one such attempt to woo the networked consumer and make him listen.

One of the facets of digital culture is corporate and technological convergence, which has now produced a seamless integration of content and advertising. The opening quote summed up the challenge that awaits a marketing expert who travels this new medium. Gamers are a strange sort, the creators, heroes and deities of their experience, at the same time shackled like no one in the real world<sup>2</sup> and with powers parallel to none. Computer games are surging to prominence in the modern media and entertainment structure<sup>3</sup> so much that there is more and more talk about

- 
1. “The touch”, of course, remains crucial. With Internet and on-demand, perhaps more than ever, content is king. However, it is imperative not to forget the means of transposition. The success of the 2010 Old Spice campaign is attributed to its’ innovative entrenching of an interesting concept into the Web 2.0 world of Twitter, YouTube and Facebook. Opening new venues for commercial messages in the sea of content is, however, a neverending story.
  2. “Code is law”, as Lawrence Lessig would say. See Lessig L., *Code and other Laws of Cyberspace*, Basic Books 1998.
  3. GameVision Europe’s 2010 study of gamers has shown that in the eight indicative nations within the EU, on average, 25.4% of adults have played a computer game in the last 6 months, 31% of all males and 20% of females. Preconception that only the young are interested is contradicted by the findings: *exempli causa*, while around 70% of the 16-19 aged population play, this figure is around 50% in the 20-29 and around 30% in the 30-44 age group, respectively. A study done for the Commission in 2006 estimated that the European market for computer games had total revenue of more than €6.3 bn, with an expected rise to €7.3 bn by 2008. PriceWaterhouseCoopers’, on the other hand, claimed that Italy, Spain, UK, Germany and France accounted for 10.9 billion euros in 2009, 30% of the global computer games market. PWC has heralded games as “the fastest growing and most dynamic sector in the European content industry”.

the “gamification”<sup>4</sup> of everyday activities. It seems that everybody plays these days – which naturally opens the door to a whole slew of connected enterprise.

The forests of advergaming are still untamed, opportunities considered abundant and possibilities of expression refreshing. Indeed, it is a tree that has been expected to bear serious fruit for a while. When the author first broached this topic, advergaming seemed like a hip, new idea. “The rise of the social networks”, the “advent of the casual gamer”, were the headlines supposed to dominate this introduction. Partially, this point still stands; however, a humbling realization, as it oft does, came with research: advergaming is hardly a completely novel concept, going as far back as computer games themselves<sup>5</sup>, rising and falling with the many waves of the industry. The difference today to these venerated ancestors lies more in scale, availability, sheer size, and the gradual shift towards the mainstream of marketing. Advergaming is growing discontent with being reserved for geeks among ad-men<sup>6</sup>. There are many reasons for such an ascent, and a deeper analysis of causes and symptoms outreaches the confines of this paper – the mentioned rise of casual gamers, expanding console network capacity, mobile gaming, massive multiplayer online games, the unimaginable explosion of Internet itself and its subsequent social phase, Web 2.0, all play a part. This leads to the conclusion that advertising in undreamt of ways, spurred by a fluid fusion of gaming, social networks and classic tricks, looms just around the corner. With opportunities for

---

4. “Gamification” is used a namer for the inclusion of gameplay mechanics in non-game applications in order to facilitate their adoption.

5. In 1973, Digital Equipment Corporation commissioned a graphical version of the game Lunar Lander from Atari, in order to demonstrate the capabilities of their new GT40 graphics terminal, in which an astronaut could order a Big Mac, or destroy a McDonalds on the Moon. In the early eighties, Kool-Aid, Pepsi, American Home Foods and several other brands developed Atari 2600 games that featured their products. In 1983, Atari had developed a special version of Space Invaders, called Pepsi Invaders – for Coca Cola. Some other examples of early full-fledged advergaming would be 7-Up’s *Spot* games (*Cool Spot*, 1993 and *Spot Goes to Hollywood*, 1995) and Frito-Lay’s *Chester Cheetah* (*Too Cool to Fool*, 1992 and *Chester Cheetah: Wild Wild Quest*).

6. The allure of the disposable income in the 18-35 male market is especially relevant. Available estimates on the growth of advergaming vary: on the low end, Parks Associates expected it to reach \$432 million by 2010. Yankee Group put the number at \$732 million for the same period, while Jupiter Research forecast \$1 billion. CEO of the in-game advertising placement company Massive Inc, had expected a rise of up to \$1.8 billion. The 2007 eMarketer report, *Video Game Advertising: Getting to the Next Level*, had suggested that advergaming would generate almost \$2 billion by 2011, mobile gaming notwithstanding.

cross-promotion<sup>7</sup> and actual acceptance of commercial content among gamers<sup>8</sup> also accounted for, future seems bright for the advergaming industry<sup>9</sup>.

Lawyers have a tendency to arrive at the scene the last, in order to play (more or less) informed catch-up and introduce order into social dynamics. This has only been confirmed in the digital age, with its inconceivable speed. After all, our vocation is, by its very nature, rooted in tradition and oft conservative rather than transformative. Small wonder, then that most of the literature on the topic was written by ad-men for the ad-men, legal texts being few and far between. However, as competing agendas<sup>10</sup> come into play in a multi-million euro industry, the question of legal certainty asserts itself – the attitude of “anything goes”, afforded by relative obscurity, poised to dissolve. The duty of the regulator is to set the rules for governing the interaction of actors in a society. Law will step in. The author will strive to be bold and go a step beyond merely displaying advergaming and associated rules, into illuminating some of the more interesting problems that may arise in the future. It is the intention of this paper to provide a glimpse into this new frontier, the perils and rewards it keeps, the paths legislation has taken so far, and serve as a call for examining a very interesting topic further.

## 2. Advergaming: Forms and Shapes

Advergaming<sup>11</sup>, fundamentally, is used to denote the promotion of products or

---

7. Creative applications, such as Capcom's cooperation with the clothing company Diesel through its *Devil May Cry* franchise or Puma's cross promotion with *True Crime: New York*, have already been tried.

8. Although this is tied to the phenomenon of immersion, according to an UK survey conducted by CNET Networks for the IAB 'a vast majority of gamers, 86%, said that they were happy to see ads placed within games if it brought down the prices they had to pay' and that they 'do not see in-game ads as intrusive'. *Gamers respond well to in-game advertising*, Jennifer Whitehead, Brand Republic, 2007, <http://www.brandrepublic.com/news/733658/Gamers-respond-in-game-advertising/>.

9. In 2006, such a statement would have been unconditional. However, several factors since then have caused a slowdown in expected growth. An IAB survey at the time showed that unless major advertisers are already familiar with an emerging format, in a harsh economic climate they are unwilling to experiment with unproven formats. However, it seems that since 2010 things are once again starting to pick up.

10. Just a brief overview of all the interests involved is impressive: game developers, publishers, retailers, advertisers, ad-brokers, ad-developers, platform vendors, gamers, consumer, child protection, privacy and various other NGOs.

11. Invention of the term “advergames” is attributed to Anthony Giallourakis, who registered the domain names *advergames.com* and *adverplay.com* in 2000. It later appeared in the *Wired's* “Jargon Watch” column in 2001 and spread out since. Nota bene: This paper uses the

brands<sup>12</sup> with or within computer games, principally through gameplay mechanics<sup>13</sup>. The monetary value charged for the content provided alongside the commercial message, the manner of access<sup>14</sup>, designated goal<sup>15</sup> or object<sup>16</sup> or the pe-

---

term “advergaming” to encompass all of the myriad forms that the fusion of advertising and gaming might take. This approach is not uniform in literature or popular depiction – some equate it synonymous with advergames alone; others use it to encompass, for instance, sponsorship of gamer tournaments, or game characters’ used in classical promotion schemes (e.g. Mario of *Mario Bros*’ fame advertising Ralston Cereal or Kraft noodles), which are not distinctive enough from traditional advertising.

12. This work mainly focuses on classical commercial ventures. However, political advergaming and edugaming, that is, use of gameplay for expression and propagation of ideas, world-views or education, will and has become a question unto itself, which we shall briefly touch on at several points. Some light examples would be *Good Willie Hunting*, an advergame deriding the extramarital escapades of former US president, Bill Clinton or *FreeRice*, which raises money for the U.N. Food Program.
13. Discussion on the terminology of these games is in itself varied and interesting. Differentiation between “electronic games”, “video games” and “computer games” shall not be considered relevant for the topic at hand. Computer game theorist Jesper Juul defined these games as “a rule-based system with a variable and quantifiable outcome, where different outcomes are assigned different values, the player exerts effort in order to influence the outcome, the player feels emotionally attached to the outcome, and the consequences of the activity are optional and negotiable.” Some systems, although colloquially considered games, do not necessarily fall within this spectrum: Linden Lab’s *Second Life* is often defined as a “virtual world”. Although a bitter rivalry exist between the so-called “serious” or “triple A” and “casual” games, with “social” games gaining a large foothold in recent years, this needs not affect advergaming at all – it can work well within all three environments.
14. They can be downloaded, played on the company’s website, or via social networks. While the online environment is dominant (and vital) today, many nutrition companies conducted campaigns wherein they gave out games as value meals’ prizes or inside cereal boxes (a notorious example was Chex Quest, a Doom clone, in 1996; both Burger King and McDonalds had such campaigns). In the eighties, some of the premier advergames were distributed by mail-order (*Tooth Protector* for Johnson & Johnson, *Kool Aid Man* for General Foods, *Chase the Chuck Wagon* for Chuck Wagon dog food).
15. To name a few: boosting brand awareness, encouraging a trial, market research (not only via metrics, explained further; car companies often track design preferences in advergames) or classic sales promotion (for instance, by offering a downloadable coupon as a reward). *Lada Racing Club* (2006) features real-life autopart and accessory suppliers’ products in the part where players tweak their vehicles. The game provides real-life pricing and suppliers’ contact information along with performance statistics.
16. Food and beverages were always dominant in this market, but virtually any commercial message has been tried – clothing (a line by Marc Ecko in *50 Cent: Bulletproof*), TV shows (HBO’s “*Maester’s Path*” for *Game of Thrones*, 2011), movies (*Avatar*, on Xbox Live, 2009), cars (Ferrari, Renault and Lotus, as early as Formula One, 1983, now everywhere, for a fee,

cularities of the mechanics themselves are irrelevant; the core of this definition is the promotion of information intended to alter certain behavior of recipients – via computer games. The value exchange involved seems simple: gamers give a brand their attention, and the brand provides an entertaining experience. The unique opportunities that distinguish this use of advertising and games from other venues are, above all, interactivity and impressiveness<sup>17</sup>, metrics<sup>18</sup>, customization and generativity<sup>19</sup>. Some of the inhibitors would be the learning curve and difficulty, platform fragmentation and low interoperability, lack of access for some categories of consumers and operational inefficiencies caused by no clear industry-wide standards. Their ultimate effectiveness as marketing tools is dependant on the particulars of a given case<sup>20</sup>.

---

of course), recording artists (*Escape the Fear*, used to promote Lilly Allen's album *It's Not Me. It's You*, 2008), even computer games themselves (a mini-game promoting Ubisoft's *Heroes of Might and Magic V*, 2006 or Bioware's *Dragon Age: Legends*, 2010).

17. Unlike other media, gaming is intrinsically goal-oriented and competitive, whether the fight is against a human adversary or a hostile environment. Players shape their own experience and are much more involved, compared to mere recipients. They can interact with a brand much more intimately and directly. As a result of the games' interactivity, players are more likely to retain the commercial message. <http://www.microsoft.com/presspass/press/2008/jun08/06-03adeffectivenesspr.mspx> A study has demonstrated that the more involved a player is in the gameplay, the less he remembers the brand placements, "Recall of Brand Placements in Computer/Video Games", Michelle Nelson, 2002. This implicates that it is harder to position meaningful content in a game, but also that if the player sees a placement during a state of high emotional involvement, it will likely be very effective. A 2009 study for NeoEdge Networks had shown that online gamers are more likely to recall brands embedded in games, partially credited to the way the eye perceives motion. This also leads to less advertising fatigue.
18. The ease of tracking ad-exposure and information gathering, and subsequent adaptation, is astounding. Websites can allow for assessment of factors such as the number of visitors, time spent, repeat visits, etc. In-game, statistics can be retrieved from the platform to rate demographic profile, behavior, needs, attitudes and preferences, measure impression rates, deduce the optimal positioning of advertisements, the player type (again with regional and other factors taken into account) etc.
19. Consumer-created content is considered a step forward in the advertising world. Machinima (the practice of making short animations and comics using game software), modding and skinning all fall into this category, but this represents only the tip of the iceberg. Chrysler partnered with the developers of *The Movies*, making all vehicles in the game bear its brand, and submissions for the Chrysler's "The Movies Virtual Film Competition" in 2006 featured the company's cars. Player-made Coke machines can be found in many bars in *Second Life* and an entire Ikea furniture collection had been uploaded o the *Sims Online*.
20. Gurău Călin identifies these "effectiveness factors" as accessibility, difficulty of understanding, competitive level, relevance for the object, capacity to induce and maintain the state of

In order to bear the ramifications of an intervention, one must first understand the beast he is trying to tame. We shall try to do this by briefly going through the various modalities, especially between the two core ones: advergaming and in-game advertising. Caution is advised: advergaming is by its nature a hybrid creature, fluid and unimpressed with strict boundaries and clear-cut definitions. In many cases, the difference between named concepts may be blurry indeed<sup>21</sup>.

Advergaming are computer games specifically designed and developed for the sole purpose of serving as vessels for marketing content, utilizing gameplay to facilitate the adoption of a commercial message. This *raison d'être* distinguishes advergaming from other advergaming and, based on certain given factors, presupposes some ways in which they are used<sup>22</sup>. In recent periods, most advergaming are provided free, online, with a strong drive towards social gaming<sup>23</sup> and simplicity<sup>24</sup>. For the advertiser, their comparative advantages are interactivity<sup>25</sup>, flexibility<sup>26</sup>

---

flow and viral marketing capacity.

21. "It is unclear, for instance, if the Austrian and Swiss public service broadcasters' 2008 *Ski Challenge* qualifies as an advergaming, a sponsored MOG (multiplayer online game), or a MOG featuring the placement of many products, such as various ski resorts, banner ads alongside the slope, logos on the ski-suits, and, most importantly for the broadcasters, the live broadcasting of the "real" race.", *Advertising in Online Games and EC Audiovisual Media Regulation*, p. 9, Thomas Steiner.
22. For a reasoned comparison between demonstrative and illustrative advergaming, see [http://advergamingtoday.blogspot.com/2006\\_04\\_01\\_archive.html](http://advergamingtoday.blogspot.com/2006_04_01_archive.html).
23. This significantly cuts down on transfer costs, and ensures a large diffusion, enticing players to participate and adding to the viral component, a coveted element for advertisers in Web 2.0. An advergaming that utilized this aspect was developed for GAP, where players could dress their avatar and notify friends.
24. "Serious" advergaming are rarer due to high development costs, distribution complexities and the problem common for advergaming in general - they need to fight for consumer attention with other games. Although it is possible for several complementary, non-competing brands to pool resources and showcase together, such advergaming remained a luxury affordable only to the largest few, and still mostly in the sports arena. Some of the more recent examples would be Volvo's *Drive for Life* for Xbox (2005), *World Racing* for Xbox (2003), Burger King's *King games* (2006). An interesting cross media experiment was the development of *50 Cent: Bulletproof* (2005). There are also advergaming virtual worlds, such as Disney's *Virtual Magic Kingdom* or the *Neopets.com* virtual pet community (which, compared to *Second Life*, can be used to nicely demonstrate the difference between advergaming and in-game advertising).
25. They are by definition on-demand and participatory, contrary to involuntary and passivizing.
26. They can be developed for IM applications, mobile devices, web sites, Facebook applications, widgets etc. On the low end of the budget, the most basic ones are built into banners and pop-ups, from *Orbitz* to *Shoot the Rapper* (a pop-up game that caused litigation against Traffix Inc. by rap artist Curtis Jackson, alias 50 Cent) but even on the simple front, there are

and ease of customization to the target audience<sup>27</sup>, no multi-tasking<sup>28</sup>, simplicity and speed of the development cycle, cost-effectiveness<sup>29</sup> and a potential for strong viral marketing<sup>30</sup>.

In-game advertising represents advertising embedded into the virtual environment, but in a way secondary to gameplay itself. This is a crucial factor – unlike advergames, whose whole point is to promote the product, the commercial content here is not supposed to affect the key elements of the game<sup>31</sup>. In-game adver-

---

more complex executions such as a customizable shooting scroller for Microsoft or a trivia mini-game for Sony's PlayStation.

27. Both pre-release and post-release. On the one hand, it is relatively easy to differentiate various games depending on a segmented market. Although targeting is even easier with in-game advertising, the philosophy of modern social, simple games itself is "design by feedback", so it is easy to add new content based on consumer demand, or integrate player-made content. For example, Pepsi developed an interactive microsite with an online contest, which offered downloads. Because music videos were favored four-to-one, more were added, and daily user stats grew by 100 percent.
28. Traditional advertising suffers from averting the recipient's attention from the desired content. In order to avoid this, the recipient multitasks during the commercial break, e.g. getting a snack.
29. This is a relative feature, as noted above, based on the type, complexity, effort input e.tc. In general, however, advergames are estimated to be several times cheaper, with hosting and distribution costs minimal, greater consumer retention and exposure compared to traditional counterparts. Studies have shown that the typical player may replay an *advergame* 15 times or more (Pereira, 2004) and that average time spent in an advergame is 7 to 30 minutes (Călin). Estimates suggest that when development costs are spread across players, an advergame can cost less than \$2 per a thousand users (Pereira, 2004).
30. The traditional, friendly word of mouth can enflame cyberspace in mere seconds through social networks, the blogosphere etc. Studies have shown that 90% of the players participate because of challenge links, e-mails sent by friends or word of mouth. A survey conducted by Jupiter Media Metrix reveals that 86% of Internet users passed the information about a good game to other persons and 49% passed it to more than three persons. This makes "seeding" games a necessary activity.
31. The keyword here is not particularly the storyline itself, the mechanics or the visuals, but immersion, a combination of factors that induces the player's willingness to treat the game elements as actual events, his emplacement within the virtual environment, and ability to "become" a character. Immersion is closely related to suspension of disbelief, or the willingness of players to suspend their critical faculties to the extent of ignoring inconsistencies. As long as immersion is not challenged, if an advertisement "fits" the context of a game and its unique setting, this enhances the reality factor, and the players are willing to accept advertising. The movie *Deuce Bigalow: European Gigolo* has no place in the sci-fi themed *Planetside*, but Nuka Cola, drank in the post-apocalyptic wastelands of *Fallout*, works. Verdashko suggests that using "fake brands", allusions on popular brands adds to imagination and entertainment



tising integrates a brand into a *pre-existing* narrative. At first, the technology allowed only for static<sup>32</sup> advertisements. However, Internet connectivity has made it possible to display and adapt in-game advertisements real-time, dynamically<sup>33</sup>, with especially interesting activities conducted in virtual worlds<sup>34</sup>. It can also include the more common product placement<sup>35</sup> or sponsorship<sup>36</sup> mechanisms. The benefits revolve on access to gamers (especially the young in the population), use of gameplay mechanics and immersion, and the possibility to tap into the creative well of consumer-generated content. However, there are problems with this advertising, as well – competition with other computer games, the sales mar-

---

value of the game, and advises advertisers to use proxy brands, equipped with strong but non-binding associative links to real-world originals, to build a memorable presence, similar to the Sprunk drink (Sprite) or Cluckin' Bell (Kentucky Fried Chicken) in *GTA: San Andreas*.

32. Traditional posters or billboards within an environment, but also advertisements that appear during loading screens or around game menus. The important part is that these are long-term, planned placements, hard-coded during development. Some examples would be a Shell-branded station in *Test Drive Unlimited* (2006) or the appearance of McDonald's and Coca-Cola in *Doom 3* (2004). AXE had used the medium's interactivity by providing an obstacle for the gamer to overcome in *Splinter Cell: Chaos Theory* (2005).
33. By updating the code with additional features, advertisements can change through a feedback channel. Besides adapting the chosen messages shown, this can be used for tailoring the message according to the specific player: his location, the weather conditions, the time, length of play or any number of factors. Video commercials can be displayed on a building in a virtual city, and even interactive game kiosks can be incorporated within another game. T-Mobile's appearance in EA's *Battlefield 2142*, Massive's Cadbury Crème egg campaign performed over several titles in 2009 or billboard ads featuring then US presidential candidate Barack Obama in October 2008 in *Burnout Paradise* represent such advertising.
34. There are numerous promotional examples inside open worlds, like *Second Life*. American Apparel had opened a store there (which even suffered an attack by a terrorist group, "*Second Life Liberation Army*" *Targets Brands*', MarketingVOX, 2006), MTV ran fashion shows and had bands regularly perform, Toyota used its Scion City for market research and promotion etc. Closed and advertising-dedicated virtual worlds can essentially be considered adver-games, as mentioned.
35. Product placement works a lot like placement in standard audiovisual media, with opportunities for integrated brand messaging and use of products or services by the characters. Electronic Arts contracted with Intel and McDonald's for *The Sims Online*, and Activision with Nokia for *Kelly Slater's Pro Surfer*. Lara Croft drove a Jeep Wrangler in *Lara Croft Tomb Raider: Legend* (2006), as part of a movie/game cross-promotion.
36. Notorious examples are more political in their nature: *America's Army*, sponsored by the recruitment office of the United States military, and *Special Forces*, developed for the Islamist group Hezbollah. An advertiser may particularly sponsor additional content, special features etc.

gin<sup>37</sup>, costs of development and preparation<sup>38</sup> and lackluster use of the medium's unique properties<sup>39</sup>. In 2006, the advent of advertising networks<sup>40</sup>, that had the capacity to spread a message across different titles, thus lowering transaction costs, was expected to alleviate some concerns and usher in the halcyon days of in-game advertising. However, the economic situation and competition from other forms of interactive advertising (including social advergames) had left the field worse for wear, and its' future less than certain.

### 3. The Law

After this cursory overview of basic forms of advergaming, the pertinent questions become those of the values and the manner in which regulation is supposed to in face of a challenge, in this case, from these advertising hybrids. Media services, and games in particular, hold a far too substantial economic<sup>41</sup> and cultural significance, one only likely to increase, for the law to overlook them<sup>42</sup>. The

---

37. The AAA games rely on blockbuster sales as does the movie industry, 90% titles fail to break even.

38. This is the reason why static ads were mostly unviable *en masse*.

39. The main sinners are insufficient integration with the plot and little interactivity. Content-related decision-making is programmed directly into games and should be used accordingly. Billboard ads suffer from similar problems as do their real-world analogs, maybe even more due to the player's concentration on the content. A product placement may help the player (Red Bull power-ups, *Worms 3D* or Alfa Bank ATMs in *Night Watch*), act as a reward (Pepsi's Pepsiman, *Fighting Vipers* or Burger King's King, *Fight Night Round 3*, common in racing games, as well, with branded cars), a plot point (Puma sneakers, *True Crime: New York City*, Sony Ericsson phones, *Splinter Cell: Pandora Tomorrow*, Visa credit card, *CSI: 3 Dimensions of Murder*), or a cheat code (*NASCAR 2005: Chase for the Cup* or Pizza Hut in *Everquest II*).

40. The notable players being Exent, IGA, Double Fusion and Google-owned Adscape Media. Using dynamic advertising was expected to significantly cut down production costs, time and increase the longevity of a campaign. However, the profits did not seem to materialize: Microsoft had shut down its Massive division (formerly Massive Inc) late 2010, in part because of the advertising potential of Xbox Live. The paradox is that in early 2010, in-game advertising had a comeback, as *Alan Wake* came out, loaded with brand name product including Verizon, Ford, Duracell and Energizer. CNBC.com, 2010. [http://www.cnbc.com/id/37274199/Microsoft\\_Reaps\\_Benefits\\_of\\_In\\_Game\\_Advertising](http://www.cnbc.com/id/37274199/Microsoft_Reaps_Benefits_of_In_Game_Advertising).

41. "As companies provide real services inside virtual worlds, such as employment and investment opportunities, they could draw attention - and regulation - from real-world authorities like the courts and legislatures.", BusinessWeek, [http://www.businessweek.com/magazine/content/06\\_18/b3982007.htm](http://www.businessweek.com/magazine/content/06_18/b3982007.htm).

42. Thomas Steiner identifies economic welfare and the interests of the internal market for media and entertainment content as the principal economic, and privacy and cultural diversity, especially freedom of information, opinion and expression, and consumer protection,

growth in scale and importance of gamers and the industry, and the need for a uniform approach EU-wide may mean that, while a nascent field should be encouraged to evolve on its own, a necessity for a clear, unambiguous framework and legal certainty, will rise over time.

It is vital to note that, due to its' mixed origins, both rules governing computer games as such *and* advertising and media law might apply to advergames. Depending on the *ratio legis*, rules designed to protect competition<sup>43</sup>, information flow, privacy and consumer protection may also come into play. Localization, access issues and the stated policy of propagating European works provide their own trials<sup>44</sup>. Some of the more celebrated characteristics of advergames pose certain legal problems. While advertisers and affiliated commercial interests are overjoyed by the possibility for effective metrics, especially with in-game advertising, the possibilities of using IP addresses for behavioral targeting and gamer profiling constitutes a threat for privacy advocates<sup>45</sup>, one covered by the 95/46/EC Data Protection Directive. A special concern exist for minors, whose informed

---

as the main cultural reasons for regulation. Advertising in Online Games and EC Audiovisual Media Regulation (2008), NCCR Trade Regulation Working Paper n. 2008/3, available at <http://papers.ssrn.com>. Advergames may play a part in enhancing public awareness and media literacy, notable goals of the EU legal and policy documents.

43. For instance, gatekeeping or bundling issues, or vertical dominant positions by the advertising networks.
44. "Without intervention it is inevitable that country markets outside the big five games markets in Europe will continue to be left out with regards to content localisation.", *Interactive Content and Convergence: Implications for the Information Society*. A study for the European Commission (D6 Information Society and Media), by Screen Digest Ltd, cms Hasche Sigle, Goldmedia Gmbh, Rights com Ltd, <http://ec.europa.eu>. The report also recommends various policy approaches for increasing consumer-enabling technology, such as broadband penetration and 3G mobiles.
45. The DPD defines personal data as any information pertaining to an identified or identifiable natural person, and puts forth requirements for properly informed consent, while granting specific rights to data subjects. The question of the relation of the fundamental right to privacy, as envisioned by the International Covenant on Civil and Political Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the legitimacy of controller's interests in lieu of Article 7 of the DPD would be an interesting arena to try advergames as a platform. There are other issues, such as the question of proper information and protection of minors. Google currently holds the patent for target advertising in computer games: USPTO Patent Application No. 20070072676, 'Using information from user-video game interactions to target advertisements, such as advertisements to be served in video games for example', assigned to Google Inc, invented by Shumeet Baluja, filed 29 Sept. 2005, and published 29 Mar. 2007.

consent to data collection and retention in the name of market research is dubious at the very least, even under traditional contract law, let alone the existing practices of widespread negligence and legally ill-advised behavior.

As far as content control is concerned, first of all, a paradox. In the area of copyright, piracy is generally not a concern with advergaming<sup>46</sup>. Instead, there are intellectual property issues and questions of equity in the division of rights regarding consumer-generated content and effort harnessed, with game publishers claiming sweeping rights on any third party in-game creations, contractually, through the adhesive terms of use<sup>47</sup>. Further on, content regulation, usually in the name of protecting minors from violence and pornography<sup>48</sup>, is seen by many as the impending future for virtual environments<sup>49</sup>. A greater threat still might be self-censorship and the necessity for business interests, which drive the industry forward, to put on a "presentable image". While one side of the aisle may cry

---

46. The advertising message can be transmitted whether or not the game itself was pirated. In addition, as mentioned, the bulk of advergaming today are provided free of charge.

47. Neopets.com, a site primarily catering to children, has terms that require the players to agree to: "Automatically grant...to Neopets a perpetual, royalty-free, irrevocable, nonexclusive right and licence to use, reproduce, modify, adapt, publish, translate, create derivative works from and distribute such materials or incorporate such materials into any form, medium or technology (now known or hereafter developed or devised) throughout the universe", Kids' Ad Play: Regulating Children's Advergaming in the Converging Media Context, Sara M. Grimes. Although *stricto censu* unrelated to advergaming, EA, whose *Spore* creature creator was a big hit in 2008, is another interesting example: "In exchange for EA enabling your contribution of Content, when you contribute Content to an EA Service, you expressly grant to EA a non-exclusive, perpetual, worldwide, complete and irrevocable right to quote, re-post, use, reproduce, modify, create derivative works from, syndicate, license, print, sublicense, distribute, transmit, broadcast, and otherwise communicate, and publicly display and perform the Content, or any portion thereof, in any manner or form and in any medium or forum, whether now known or hereafter devised, without notice, payment or attribution of any kind to you or any third party. You grant EA all licenses, consents and clearances to enable EA to use such Content for such purposes. You waive, and agree not to assert any moral or similar rights you may have in such Content." On the other hand, *Second Life*, the epitome of user-generated content, empowers creators through technology to limit distribution and modification of their wares by marking them with the "no copy", "no modify", or "no transfer" flags.

48. In addition, while some EU jurisdictions strive to severely regulate online gambling, free poker sites, supported by advertising, continue cropping up.

49. Children truly are a vulnerable group in advergaming. It is unlikely that they fully comprehend online business practices and are able to differentiate between media content and marketing, but they are targeted in particular, and effectively so, by fast food and soda companies. Because children are spending more time online, advergaming is a very effective way for marketers to reach and hold their attention, <http://www.expressindia.com/news/fullstory.php?newsid=36180>.

censorship, from a legal standpoint, in this field, the use of advergaming reflects a trend of integrating marketing, that is, a fundamentally commercial cause, into an area traditionally granted higher protection through freedom of speech and expression<sup>50</sup>, whereas the courts have in general been more restrictive with regard to business endeavors. This fragile line surrounding freedom of speech has already been tested in regards to discrimination, as well<sup>51</sup>. In the face of all these issues, the European regulator did not opt for the route of direct content control<sup>52</sup> so far, preferring to encourage classification primarily through the unified industry led Pan European Games Information age rating system<sup>53</sup>, administered by the Interactive Software Federation of Europe, which induces a rating scheme and upholds consumer information. It is generally adopted and considered adequate in most member states, however certain segmentation does seem to be forthcoming, with steps taken in favor of content control in national legislation<sup>54</sup>. A firmer

- 
50. A series of federal cases in the US (*Interactive Digital Software Association v. St. Louis County*, *DOOM*, *Mortal Kombat*, *Wilson v. Midway Games Inc*, *House of the Dead*) have deemed computer games protected speech, akin to books and movies. Freedom of speech applies to both the developers and gamers, whom would not have the possibility to access content. Under the logic employed, games are considered as such only if they possess certain characteristics: such as narratives, themes, and dialogue, or well-developed visual and musical components resembling those found in other forms of protected speech. Under this reasoning, rudimentary games, such as the majority of advergaming today, would not hold these privileges. *Grand Theft Ore: The Constitutionality of Advergame Regulation*, Seth Grossman.
  51. A prime political example being the game which the Swiss People's Party provided on its website before the October 2007 elections, enabling players to kick black sheep out of the country, while protecting white sheep from "evil" immigrants, <http://www.zottel-game.ch/>.
  52. Rare and isolated incidents of banning games in certain member states did occur, a notable case being *Manhunt 2* in UK, Ireland, Germany and Italy.
  53. Although there was a push for stricter rules and measures in 2006 and 2007 by Justice and Security Commissioner Franco Frattini and the German Presidency. <http://www.euractiv.com/en/infosociety/violent-video-games-ban-self-regulation/article-159911>, PEGI and PEGI On-line have remained the chief operation in place Europe-wide.
  54. Germany is not a member of PEGI, but has an autonomous, state-controlled system, which has been criticized for its stringency (especially the "harmful media index"). Some member states have been aiming at a classification for distribution, circulation and advertising based on an age/content rating (Italy, UK, Germany, Estonia, Greece, Latvia, Lithuania and Slovakia). France, Sweden and the Netherlands prohibit certain violent games under criminal law (in Sweden constitutional law, even). In Belgium and Malta, there are a number of legal provisions covering the sale of computer games, such as laws on racism and xenophobia, commerce, consumer protection and public order. *COM/2008/0207, Communication from the Commission on the protection of consumers, in particular minors, in respect of the use of video games*.

guideline, improved dissemination, development and enforcement in practice, maybe even community-level hard law that would hold a liberal and unified approach (not necessarily by giving surveillance and monitoring powers to governmental structures) may be desirable and could encompass advergaming.

On the advertising front, Directive 2010/13/EU, commonly referred to as the Audiovisual Media Services Directive, is considered the premier legal framework. However, the wording leaves questions on whether or not computer games, especially online games, are included under the rules. Recital 22 explicitly rules out “[...] games of chance involving a stake representing a sum of money, including lotteries, betting and other forms of gambling services, as well as on-line games and search engines[...].”<sup>55</sup> While recitals are indicative means of interpretation, they are not part of the enforceable text of the directive. The idea of regulating advertising is explicitly not intended to be lenient towards “new” forms of media<sup>56</sup>. It would be interesting to have a court examine this issue; however, a deeper analysis of the relevant provisions seems to put advergaming into an audiovisual media service context. It is by its nature on-demand, or non-linear, in the wording of the Directive. It can be interpreted to fall under “a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, under the editorial responsibility of a media service provider and the principal purpose of which is the provision of programmes<sup>57</sup>, in order to inform, enter-

---

55. The reasoning given – the incidental nature of audiovisual content, does not hold water for advergaming. Such wording has been branded a result of lobbying efforts by the Interactive Software Federation of Europe and other players in the industry, e.g. Microsoft. In a submission to the EC in June 2006, the ISFE urged the exemption of online games from the application of the AVMS Directive. Major reasoning was that, because the plot of the game is unscripted and AI is present, online games (in general) are about user created content and that the “general public” is not provided with but *creates* the content. Therefore, it is “impossible to affix editorial responsibility to one particular natural or legal person”, since participants are “constantly reorganizing and creating content in the form of everchanging identities, ad lib chat, etc. While this is true to an extent for some games, it is hard to claim so for a significant part – advergaming included – and for quite a few advertising practices, solely by virtue of venue, do not fall under this umbrella. *Advertising in Online Games and EC Audiovisual Media Regulation*, Thomas Steiner, 2008.

56. “The availability of harmful content in audiovisual media services is a concern for legislators, the media industry and parents. There will also be new challenges, especially in connection with new platforms and new products. Rules protecting the physical, mental and moral development of minors as well as human dignity in all audiovisual media services, including audiovisual commercial communications, are therefore necessary.”

57. Contrary to the claims of the ISFE, the requirements of Article 1 for existence of effective control over the selection and organization of programmes, meaning individual sets of moving

tain or educate, to the general public by electronic communications networks<sup>58</sup> (audiovisual media service in general). But also, “images with or without sound which are designed to promote, directly or indirectly, the goods, services or image of a natural or legal entity pursuing an economic activity, which accompany or are included in a programme<sup>59</sup> in return for payment or for similar consideration or for self-promotional purposes” (audiovisual commercial communication). The requirement of making available to the public via electronic communication networks would limit advergames coverage to online-distributed content alone; however, with new business models, this should be less of an issue. This approach would mean that the rules of AMSD are valid for the situation, especially Articles 5-13. Problems with advergames in practice might arise from the transparency principle and the ban on surreptitious advertising<sup>60</sup>, restrictions on alcohol and tobacco advertising, and especially children-targeted limitations<sup>61</sup>. Handling advergames in a manner significantly different from the Directive in

---

images with or without sound, within a catalogue established by a media service provider, the form and content of which are comparable to that of television broadcasting, simply is the state for most advergames content. A pertinent question and a subject for deeper analysis might be: who, out of the numerous stakeholders, asserts this control and in what capacity? It need not even be focused on a particular natural or legal entity, but shared along the lines. This would depend on the advergame at hand, and is utterly different for advergames and in-game advertising. As for the required “television-likeness”, there are grounded assertions of similarity between games and movies. *Advertising in Computer Games*, Ilya Vedralshko.

58. Within the meaning of point (a) of Article 2 of Directive 2002/21/EC: “transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed”.
59. An analysis and appropriateness of this “companionship” and “inclusion” in the case of a hybrid is compelling. However, gameplay is more relevant in the definition of advergames than the images themselves. AVCC was designed to be as encompassing as possible, while excluding radio, and this shows.
60. How is one to separate entertainment from commercial content in a perfect mishmash of both? Recital 81 holds that “the principle of separation should not prevent the use of new advertising techniques”.
61. While advertising unhealthy food is delegated to a recommendation for encouraging media providers to develop codes of conduct, Article 9, (g) clearly forbids abuse of the child’s vulnerable status.

lieu of sponsorship<sup>62</sup> and product placement<sup>63</sup> is hard to imagine. It should be noted that the fragmentation of rules regarding product placement, with member states being allowed to introduce stricter regulation in certain cases, can not be beneficial for legal certainty and development of the internal market.

Other common provisions must be observed, and here another floodgate of directives opens. When introducing an advergame, care should be taken of both Directives 2003/33/EC on tobacco advertising, and especially 2006/114/EC on misleading and comparative advertising, which sets precise standards for sanctioning advertising that can be considered misleading<sup>64</sup> and rules on permitted, though very regulated, comparative advertising<sup>65</sup>. Related consumer protection rules are also important, especially unfair commercial practices, as regulated by the Directive 2005/29/EC (which can be utilized in an advergaming environment without greater difficulty) and the 2000/31/EC e-commerce Directive<sup>66</sup>. Of course, seeing as how most of the subject matter is covered by directives, national provisions that transpose them come to the forefront.

---

62. Media law generally distinguishes sponsorship and advertising by underlining the difference in promoting a specific product or brand, versus financing a programme without being part of the creative process. The Directive names sponsorship as any contribution made by public or private undertakings or natural persons not engaged in providing services or producing audiovisual works, to the financing of audiovisual media services or programmes. This must be done with a view to promoting their name, trademark, image, activities or products and can easily be applied to advergaming.

63. The regime of AMSD has somewhat liberalized product placement. Examining it from an advergaming perspective would surely be fruitful. It defines it as 'any form of audiovisual commercial communication consisting of the inclusion of or reference to a product, a service or the trade mark thereof so that it is featured within a programme, in return for payment or for similar consideration'. In-game product placement, thus, yields an abundance of legal questions and is a very shaky ground.

64. "any advertising which in any way, including its presentation, deceives or is likely to deceive the persons to whom it is addressed or whom it reaches and which, by reason of its deceptive nature, is likely to affect their economic behaviour or which, for those reasons, injures or is likely to injure a competitor". Criteria for determining misleading advertising is also set, and includes the characteristics of goods or services, the price and the advertiser himself.

65. There are quite a few factors involved, mostly related to making the comparison as informative, fair and objective as possible. Pepsi Wars would probably not have passed the requirements of this directive.

66. Especially Articles 6 and 7, on regulating commercial communication through an information society service and an opt-in system for unsolicited commercial communication (a bit less relevant, since advergames are demand-driven, but could pop up, pun intended).



There are several contentions that may be drawn from this overview. There is a great amount of regulation partially concerning the subject matter, but it is diffused and segmented, somewhat complementary, somewhat supplementary. It is not really properly geared to the topic of discussion, even if found applicable in a concrete case. Indeed, for the most part, it does not take it into consideration. This leads to legal uncertainty and offers gamers, but also, industry interest, less protection than intended by the regulator. Neither does adequate court practice, so far, exist to light the way. Enhanced coordination and integration into a fully-fledged regime is imperative.

#### **4. Conclusion**

Advergaming is a relatively new, inspiring commercial frontier. This fusion of entertainment, creative expressionism, technical prowess and mechanics has its roots and consequences in the social structure and the norms that try to steer it. It came on the wings of global interconnection and gaming turning mainstream, and there is no reason to think it will vanish any time soon. Emerging business practices often elude outdated regulation and codes of conduct, and whispers of game legislation have focused, at least up to now more on hot button, short-term expedient topics, mainly computer-game related violence. The question for policymakers, regulators, and judiciary, whether dealing with editorial responsibility of advergame providers or the validity of data-mining practices, to ask themselves is about control – who has the capacity to make important decisions, and who stands to gain from them? In some forms, the central creative work is initiated and sculpted by a third party, a game developer or publisher, and the advertiser is the one who begs entry. In others, it is commissioned and controlled by the advertiser himself. It is doubtless that the rewards for wise utilization of these tools shall be plentiful, but a system for equitable sharing of the benefits must be established. In order to do so, lawyers must examine, acknowledge, respect and adapt to the state of the field.

How much regulation is enough? We have seen some of the affected interests, shed light on a few actors and shapes. Are private regimes and the industry itself capable enough to be trusted with the future of advergaming? Should the advertising, gaming, and interactive software industry extend its codes of conduct in order to substitute or complement regulation and soft law and recommendations be deemed sufficient? While they are more expedient, in order for any self-regulatory system to truly work in the interest of citizens, independent review must be established. Is this co-regulation the way forward? What would an act, authentically devised to be inclusive and straightforward towards gaming, look like? Moreover, how much room would there be for hybrids such as advergaming?

A regulatory challenge is brewing. Infusion of advertising funds may bolster the computer game industry to unprecedented heights and provide consumers with prime content. The gamification of advertising can only be expected to increase in innovative ways the benefit of all the market players. Advertising itself has been regulated. Yet, the framework in which advergaming is supposed to operate is complex, interwoven, often treacherous and fragmented, with scarce regard paid to the nascent medium. At some points, it is found wanting; at others restrictive. Do the rules preserve culture, property and privacy or do they not? Gaming laws need not threaten freedoms, profitability or the creative potential. Clear and comprehensive regulation, crafted with knowledge, care and understanding of the medium's particularities, may foster dialogue, improve market certainty and confidence, foster development and provide reasoned and firm guarantees for some of the issues ahead. A gaming charter.

Gamers, a quarter of European population, watch the future anxiously. Their experiences may hang in the balance. For now, this is uncertain. Advergaming is still under the radar. Anything goes. Let it not be forgotten that in advertising, as in computer games, context rules.

## 5. References

*Advertising in Online Games and EC Audiovisual Media Regulation*, Thomas Steiner, 2008, NCCR Trade Regulation Working Paper n. 2008/3 available at <http://papers.ssrn.com>

*Grand Theft Ore: The Constitutionality of Advergame Regulation*, Seth Grossman, 2005.

*Advertising in Computer Games*, Ilya Vedrashko, 2006.

*Brand Placements in Computer and Video Games: An Overview and Research Questions*, Kerri Kuhn, Anita Love & Nigel K. Ll. Pope, 2004.

*It's child's play: advergaming and the online marketing of food to children*, Elisabeth S. Moore, Kaiser Foundation, 2006.

*Video Gamers in Europe 2010*, GameVision Europe, prepared for the Interactive Software Federation.

*AdEx 2008: European online advertising expenditure*, Interactive Advertising Bureau Report, 2009.

*Game Advertising Platform Status Report: LET THE GAMES BEGIN*, Interactive Advertising Bureau, 2007.

*Interactive Content and Convergence: Implications for the Information Society*, Screen Digest Ltd, CMS Hasche Sigle, Goldmedia Gmbh, Rightscom Ltd, prepared for the European Commission, 2006.

*The Media in South-East Europe - Comparative Media Law and Policy Study: European Media Law and Policy Framework*.

*Advergaming: characteristics, limitations and potential*, Gurău Călin, 2009.

*Advertising 2.0: Social Media Marketing in a Web 2.0 World*, Tracy L. Tuten, 2009.

*Adertainment or Adcreep: Game Players' Attitudes towards Advertising and Product Placements in Computer Games*, Journal of Interactive Advertising, Michelle R. Nelson, Heejo Keum, Ronald A. Yaros, 2004.

*An Analysis of the Video Game Regulation Harmonization Effort in the European Union and Its Trans-Atlantic Chilling Effect on Constitutionally Protected Expression*, B.C. Intellectual Property and Technology Forum, Kyle Robertson, 2008

*Kids' Ad Play: Regulating Children's Advergaming in the Converging Media Context*, Sara, M. Grimes, International Journal of Communications Law & Policy, 2008.

*Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)*

*Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising*

COM/2008/0207, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the protection of consumers, in particular minors, in respect of the use of video games

*Plug (the Product) and Play: Advertisers Use Online Games to Entice Customers*, Washington Post, Ellen Edwards, 2003.

*Game Regulation: Where are we now*, Gamasutra, Niels Clark, 2009, [http://www.gamasutra.com/view/feature/3907/video\\_game\\_regulation\\_where\\_we\\_.php](http://www.gamasutra.com/view/feature/3907/video_game_regulation_where_we_.php)

# **The Google library project and its international dimensions**

---

---

**Antigoni Trachaliou**

---

---

## **Introduction**

The Google Library Project (GLP), one of the most colossal as well as debated projects of digital mega-owner Google, is in position to change the pivot of the copyright ecosystem by redefining the fair use doctrine and affecting digital copyright protection internationally. Opponents of Google's radical project confront with hesitance a plan based on the "so sue me" basis and demand that Google goes back to negotiating like any other publisher. From this conservative point of view, the existing copyright systems should be preserved, and can be adapted into the digital epoch. From another point of view however, there are those who believe in Google's good-will in pursuing something more than economic benefit; pursuing a higher cause such as the facilitation of the dissemination of knowledge online. The same people regard the demand to rely on the old ways as outdated and underline that they cannot foster progress. The question remains: should a project that will undeniably multiply the educational and cultural benefits of worldwide circulation of books through the internet, in an era characterized by the digital dominion, be held back due to the inefficiency of copyright legislators to protect right holders through the currently operating copyright system? In my opinion, the time has come to restructure digital copyright protection.

## **The Google Library Project description**

The GLP was announced on December 2004. The Project was one of Google's most ambitious plans and has been faced with both enthusiasm and skepticism as is every innovative idea that involves more than one stakeholder. The GLP, also referred to as the "scan first-ask later project" is a project promoting the creation of a digital library without the need of copyright licensing in its traditional sense; vigorously based on the fair use argument and the need to promote access to books in an environment which by nature was until now thought to undermine it. The digital library will be created by scanning books belonging to some of the

world's largest American and International libraries<sup>1</sup> into Google's database, which in exchange will give the libraries one digital copy of every work<sup>2</sup>.

In response to every search query the user will be able to access the "snippet" related to the query and a few sentences before or after. If there are many snippets in the same book referring to the search query the user will only be able to access 3 of them at the maximum. This does not apply to books which are already in the public domain and shall be fully visible. Finally, the text of reference books will be scanned into the search database but the user will only receive bibliographical information in response to the query where the display of even snippets could harm the market for the work (ex. dictionaries)<sup>3</sup>. Simultaneously, links will enable the user to locate and buy the book directly from the seller or publisher; thus facilitating access to the entire content.

Google's effort to "digitally" exploit the book thesaurus scattered around the globe is divided in 2 projects: the Partner Program and the Library Project. However the differences between the two programs are substantial and have led to no reactions in view of the Partner Program. The principal difference is that in the Partner program, the publisher authorizes Google to scan the book and therefore digitization occurs pursuant to an agreement with the copyright owner. Moreover, in response to the user query, the user will be able to see the full page containing the term and a few pages before and after that; versus the one to three "snippet" border line for the GLP. In this sense the definition of "snippet" or the length of the annotation shown in a KWIC (key word in content) has become an issue of capital importance as it is not a legal term and controversy could rise regarding its interpretation<sup>4</sup>.

- 
1. The libraries participating so far in the Project either partly or fully are: Bavarian State Library, Columbia University, Committee on Institutional Cooperation(CIC), Cornell University Library, Harvard University, Ghent University Library, KEIO University Library, Lyon Municipal Library, the National Library of Catalonia, The New York Public Library, Oxford University, Princeton University, Stanford University, University of California, University Complutense of Madrid, University Library of Lausanne, University of Michigan, University of Texas Austin, University of Virginia, University of Wisconsin-Madison, available at <http://books.google.com/googlebooks/partners.html>.
  2. Commonly referred to as the library digital copy.
  3. Jonathan Band, The Google Library Project: both sides of the story, at 2(2006), *Plagiarist: Cross-Disciplinary Studies in Plagiarism, Fabrication, and Falsification*, 1 (2): 1-17.
  4. "The owners have argued that "snippet" is not a legal term. Therefore, at some point in the future Google could start displaying larger portions of the indexed books, which could displace sales. Google responds that if it does change its policy in a manner that hurts sales, the owners can sue at that time. Since displaying some of a book's text in response to a search query implicates both the reproduction right and the display right, an owner will be able to

### ***a. Key players- litigation- current status***

On September 2005, the Authors Guild and some individual authors sued Google in the United States District Court for the Southern District of New York<sup>5</sup>, alleging that the GLP infringed their copyrights. The lawsuit was styled as a class action<sup>6</sup> on behalf of all authors whose works were in the University of Michigan collection and the request was for damages and injunctive relief. On October 19, 2005, five publishers-McGraw-Hill, Pearson, Penguin, Simon & Schuster, and John Wiley & Sons-sued Google in the same court with the difference that they only requested injunctive relief. The two cases were ultimately consolidated into one action<sup>7</sup>. On October 2008 and in view of the precariousness of the outcome of the litigation the parties reached a settlement<sup>8</sup>. The settlement although having reached preliminary approval on November 17, 2008, caused a great deal of debate and faced negation from both the right holders and the Department of Justice (henceforth, the DOJ)<sup>9</sup>. In response to these reactions an amended settle-

---

bring an infringement action against Google when it changes its policy, even if that occurs long after the original scanning of the book. Accordingly, there is no reason to prevent Google from proceeding now, when its practices do not harm owners. It is unlikely that these fees would increase authors' incentive to write", Id at.10,available at [http://www.aaupnet.org/aboutup/issues/0865\\_001.pdf](http://www.aaupnet.org/aboutup/issues/0865_001.pdf).

5. On the 31<sup>st</sup> of March 2010 an unexpected turn was affixed on the Google books opposition. The American Society of Media Photographers and other groups representing visual artists announced their plan to file a class-action lawsuit against Google, asserting that the company's efforts to digitize millions of books from libraries amount to large-scale infringement of their copyrights as well. After the rejection of the Society's efforts to intervene in the settlement last year, it moved on to seek compensation for visual artists whose work appeared in the books and other publications which Google has illegally scanned (see Miguel Helft, Visual Artists to Sue Google Over Vast Library Project, The New York Times, Ap.6, 2010 available at <http://www.nytimes.com/2010/04/07/technology/07google.html>).
6. Class action definition: a lawsuit brought by one or more plaintiffs on behalf of a large group of others who have a common legal claim (see <http://www.answers.com/topic/class-action>).
7. *The Authors Guild, Inc., et al. v. Google Inc.*, Case No. 05 CV 8136 (S.D.N.Y.).
8. Original settlement agreement available at [http://www.googlebooksettlement.com/r/view\\_settlement\\_agreement](http://www.googlebooksettlement.com/r/view_settlement_agreement).
9. The main oppositions of the DOJ regarded the application of rule 23 referring to which they said "As a theoretical matter, a properly defined and adequately represented class of copyright holders may be able to settle a lawsuit over past conduct by licensing a broader range of conduct to obtain global copyright peace and in conformity with antitrust law", see STATEMENT OF INT. of the U.S., 05 Civ. 8136 (DC), available at <http://www.justice.gov/atr/cases/f250100/250180.pdf>.

ment<sup>10</sup> was proposed on November 13, 2009 which was also granted preliminary approval on November 19, 2009. Final approval can be granted by the judge upon realization that the settlement is “fair, reasonable and adequate” for the class members, because the suit is a class action<sup>11</sup>. The final fairness hearing on the case took place on February 18, 2010 and judge Denny Chin after something more than a year, on March 22, 2011, gave his final ruling on the settlement which was rejected<sup>12</sup>. Judge Chin pointed to the Congress for answers on several of the issues under debate. He further stated that the Court would have a status conference on April 25, 2011 which was later postponed for June 1<sup>st</sup>.

The DoJ in the final fairness hearing appeared to remain in opposition to the settlement in its amended form. William Cavanaugh Jr., Deputy Assistant Attorney General for Civil Matters, representing the DoJ characteristically said “the forward-looking business plans contemplated by the settlement may be a good idea, but they were outside the scope of the settlement. This turns copyright law on its head<sup>13</sup>”. According to the statement of interest by the DoJ, in addition to several unfair-competition issues and the remaining copyright infringement theories, the main problem of the settlement had to do with the implementation of rule 23, in particular with regard to right holders of out-of-print works and foreign right holders. The settlement “essentially authorizing, upon agreement of the Registry, open-ended exploitation of the works of all those who do not opt out<sup>14</sup>” would according to the DoJ need modification in order to comply with Rule 23. Secondly, The Parties had not demonstrated that the class Representatives adequately

---

10. Amended settlement available at [http://www.googlebooksettlement.com/r/view\\_settlement\\_agreement](http://www.googlebooksettlement.com/r/view_settlement_agreement).

11. Fed.R.Civ.P.23(e). A settlement of a class action requires approval of the court. Because Rule 23 (e) does not set forth the factor to be taken under consideration when determining when a settlement is fair, reasonable and adequate, the factors used by Judge Chin’s Circuit are the so called “Grinnelli factors”: 1) the complexity, expense and likely duration of the litigation, 2) the reaction of the class to the settlement, 3) the stage of the proceedings and the amount of the discovery completed, 4) the risks of establishing liability, 5) the risks of establishing damages, 6) the risks of maintaining a class action through trial, 7) the ability of defendants to withstand greater judgment,) the range of reasonableness of the settlement fund in light of the best possible discovery and 9) the range of reasonableness of the settlement fund in light of the attendant risks of litigation (*City of Detroit v. Grinnell Corp.* 495 F.2d 448, 463 (2<sup>nd</sup> Cir. 1974)).

12. See full decision at <http://www.nysd.uscourts.gov/cases/show.php?db=special&id=115>.

13. Google Book Search Settlement Fairness Hearing Has Concluded, Here Come the Reports, Resource Shelf, Feb.19,2010 available at <http://www.resourceshelf.com/2010/02/18/google-book-search-settlement-fairnesss-hearing-has-concluded-here-come-the-reports/>.

14. STATEMENT of INT. of the U.S, 05 Civ. 8136 (DC)at 7.

represented absent class members<sup>15</sup>. The DoJ believes no adequate notice was given which is unacceptable “given the size and geographic scope of the class, and the alteration in copyright protection that the Proposed Settlement would effectuate.”<sup>16</sup> The notice requirement is designed to ensure that absent class members are also provided with the chance to protect their rights. William Cavanaugh Jr. also noted in the hearing that “the settlement has the effect of rewriting contracts” in support of his belief that publishers and the Authors Guild do not have a right to enable a third party such as Google to use an author’s work without their permission<sup>17</sup>.

Judge Chin obviously agreed with several of the points raised by the DoJ.

### ***b) Orphan and out-of-print works***

Right holders can be divided into 3 categories for the purposes of the GLP: active right holders<sup>18</sup> (the ones that register with the registry<sup>19</sup>), inactive right holders (those who fail to opt-out of the settlement and also fail to register with the Registry including in copyright but out-of print<sup>20</sup> work owners) and orphan works. “Orphan works” refer to the subset of right holders who are unknown or cannot be located after diligent search. “The Project, from one hand brings forth unused or inaccessible books which in digital format can even be accessible to people with disabilities but at the same time establishes a marketplace in which only one competitor would have authority to use a vast array of works, especially orphan works<sup>21</sup>”.

---

15. See *Amchem*, 521 U.S. at 620, 628-29 and *Wal-Mart Stores, Inc. v. Visa U.S.A., Inc.*, 396 F.3d 96, 106-13 (2<sup>nd</sup> Cir.2005).

16. STATEMENT of INT. of the U.S., 05 Civ. 8136 (DC) at 7.

17. Google Book Search Settlement Fairness Hearing Has Concluded, Here Come the Reports, Resource Shelf, Feb. 19, 2010 available at <http://www.resourceshelf.com/2010/02/18/google-book-search-settlement-fairness-hearing-has-concluded-here-come-the-reports/>.

18. See <http://blog.librarylaw.com/librarylaw/2009/03/google-books-settlement-at-columbia-part-1.html>.

19. See p. 10.

20. “The Amended Settlement Agreement uses the term Commercially Available, which generally means that a Book is in-print. If a Book is not Commercially Available, that means, in general, that it is Out-of-Print. Google is authorized to make Display Uses and Non-Display Uses of each Book that is not Commercially Available for the term of the U.S. copyright for that Book unless the Rights holder directs Google not to do so or directs Google to remove the Book”, available at <http://www.googlebooksettlement.com/help/bin/answer.py?hl=en&answer=118704#q29>.

21. STATEMENT of INT. of the U.S., 05 Civ. 8136 (DC) at 3.



According to the amended settlement, copyright owners of out-of-print works can deny Google permission to use their works in certain ways if they learn of the agreement and their rights under it<sup>22</sup>. But, copyright owners of out-of-print works provide a release to Google for any exploitation of their rights that occurred prior to those owners becoming aware of Google's use<sup>23</sup>. In addition, "because the owners of orphan works are an incredibly diverse group that includes not only living authors or active publishers, but heirs, assignees, creditors, and others who acquire the property interest by contract or operation of law, these rights holders are difficult or impossible to locate, and thus difficult to notify<sup>24</sup>". In conclusion it is unlikely that any feasible amount of notice would be capable of alerting and protecting orphan rights holders who are unaware of their rights.

However, in response to the DoJ's concerns regarding out-of-print works and especially orphan works, the amended settlement changed Article 6.3 of the original settlement regarding unclaimed funds by a fundamental alternation of the distribution model. Before the amendment, if an out-of-print copyright owner did not come forward within five years, profits from the commercial use of the out-of-print work were to be distributed to pay the operational expenses of the Registry that were related to its performance and then on a proportional basis to the Registry's registered rights holders. "Therefore, at the expense of every rights holder who failed to come forward to claim profits from Google's commercial use of his or her own work the Registry and its registered rights holders would benefit"<sup>25</sup>. The DoJ had stressed out that the fact that out-of-print rights holders might have benefited from a fundamental alteration of their rights, is insufficient to show that they had been adequately represented by named plaintiffs whose rights would not be altered (or who could readily avoid such alteration), and who would stand to gain if out-of-print rights holders did not opt out<sup>26</sup>.

Google through the amended settlement and in response to accusations about a) negligence regarding the copyright status of orphan works as much as b) the limited breadth of the class-action representation of orphan works right holders, responded with a complete remodeling of article 6.3. The provision now holds that unclaimed funds will primarily be held by the Registry for the benefit of rights-holders of such Books until they register or claim the books. The article also provides for an up to 25% use of the "per year" unclaimed funds deriving from books

---

22. S.A. §§ 3.2(e)(i), 3.5, 4.7.

23. S.A. §§ 10.1(f), 10.1(m)-(n), 10.2(a).

24. STATEMENT of INT. of the U.S, 05 Civ. 8136 (DC) at 6.

25. Id. at 9.

26. Id. at 10.

that have remained unclaimed for at least 5 years, to favor the efforts to allocate right holders of those books. Regardless however of those provisions, Judge Sin in his decision regarding the amended settlement concluded that “the establishment of a mechanism for exploiting unclaimed books is a matter more suited for Congress than this Court”.

### ***c) The Book Rights Registry***

Under the 2008 original agreement Google took a step up and introduced the creation of a non-profit entity called the Book Right Registry whose duty would be representing rights holders and negotiating their interests in respect of the GLP by identifying and coordinating their payments. Google agreed to pay \$34.5 million to fund the launch and initial operations of the Registry and cover other Administrative Costs. In exchange for the benefits conferred in the Settlement Agreement Google, each fully participating and cooperating library and host site was authorized “(a) to make Display Uses and Non-Display Uses<sup>27</sup> of its Books and Inserts in GBS and other Google Products and Services, (b) to use its Library Digital Copy and (c) (each Host Site) to make the Research Corpus available, all in accordance with the terms and conditions of this Settlement Agreement, a Library- Registry Agreement or a Host Site-Registry Agreement.<sup>28</sup>”

The settlement also provides that any breach of the terms or conditions of the settlement would not result in the termination of such authorizations except as provided in Section 3.7 (b) (Failure to Provide Contemplated Rights holder Services). It's also interesting to notice that the first Settlement agreement neither authorized nor prohibited, nor released any Claims with respect to, “(1) the use of any work or material that is in the public domain under the Copyright Act in the United States, (2) the use of books in hard copy (including microform) format other than the creation and use of Digital Copies of Books and Inserts, or (3) the Library's Digitization of Books if the resulting Digitized Books are neither provided to Google (pursuant to the Settlement Agreement), nor included in the Library Digital Copy provided to the Library by Google, or the use of any such Digitized

---

27. Non-display Uses are uses that do not involve displaying any content from the book to the public. Examples include: bibliographic information, full text indexing without displaying the text, geographic indexing of books and algorithmic listings of key terms for chapters of books. Definition is available at <http://www.googlebooksettlement.com/help/bin/answer.py?hl=en&answer=118704> Question 36.

28. Amended settlement available at [http://www.googlebooksettlement.com/r/view\\_settlement\\_agreement](http://www.googlebooksettlement.com/r/view_settlement_agreement).

Books that are neither provided to Google pursuant to the Settlement Agreement nor included in such LDC (Library Digital Copy)<sup>29</sup>”.

Although the Registry will unavoidably be a Google sponsored project, the organizational structure of the Registry has been canvassed as one to reassure the unbiased distribution of profits. The board of directors responsible for each action of the Registry (through majority decisions) will be composed by the Author sub-class and the Publisher sub-class with several guarantees of equal participation of both in the decision making process. The amended settlement also provides for an independent “Unclaimed Works Fiduciary” empowered to act with respect to the exploitation of unclaimed books or inserts. It’s interesting to notice that Google in response to the DoJ’s criticism toward Article 4.7 of the first agreement which authorized, upon agreement with the Registry, open-ended exploitation of the works of those who do not-opt-out, amended the Article by stating that Google would give registered right holders or the unclaimed works fiduciary a 60 day notice prior to the adoption of any additional revenue model. It is apparent that Google is attempting to reinforce the impartiality and integrity of the Registry as an act of good will towards the final settlement of the project.

#### ***d) The opt-out copyright strategy and competition***

In August 2005 the so called “opting out policy” was announced as a response to the reaction by the American Association of publishers and the Authors Guild. The opting out policy, as opposed to the opting in policy adopted by all copyright systems so far, remains the corner stone of the problem posed by the GLP and the basis for those who accuse Google for audaciously stretching too far. The opting out policy refers to the opportunity given to copyright owners to expressly decide not to participate in the project by providing a list with the titles they do not want to be included, regardless of whether or not they are within the libraries whose books are to be digitized. In-copyright books would not be digitized within the period from August 2005 to the 1<sup>st</sup> of November 2005. With the first settlement, which did not apply to books first published after January 5, 2009, the deadline to opt out was extended to September 4, 2009<sup>30</sup> and with the amended settlement the deadline to opt-out, object or opt back into was set for January 28,

---

29. Attachment B1 to SA available at [http://static.googleusercontent.com/external\\_content/untrusted\\_dlcp/books.google.com/en/us/booksrightsholders/Attachment-B-1-Library-Registry-Agreement-Fully-Participating.pdf](http://static.googleusercontent.com/external_content/untrusted_dlcp/books.google.com/en/us/booksrightsholders/Attachment-B-1-Library-Registry-Agreement-Fully-Participating.pdf).

30. Updated notice available at [http://static.googleusercontent.com/external\\_content/untrusted\\_dlcp/www.googlebooksettlement.com/en/us/Final-Notice-of-Class-Action-Settlement.pdf](http://static.googleusercontent.com/external_content/untrusted_dlcp/www.googlebooksettlement.com/en/us/Final-Notice-of-Class-Action-Settlement.pdf).

2010<sup>31</sup>. If one had opted out of the Original Settlement and wished to remain opted out, there was no need to opt out again and unless they had been withdrawn, objections filed to the Original Settlement needn't be refilled<sup>32</sup>.

Opting out according to Google means as explicitly stated in its site<sup>33</sup> "that the author or publisher is retaining all rights to bring a legal action against Google, for digitizing and displaying the author's or publisher's books and Inserts, and against the Participating Libraries, if desired. It also means that the settlement neither authorizes Google to make certain uses of these books and Inserts nor does it prohibit Google from doing so". The author or publisher by opting-out can request that the Settlement Administrator ask Google not to digitize or display any contents from the books or Inserts<sup>34</sup> identified in the opt out form."Although Google has no obligation under the Amended Settlement to comply with such request, Google has advised the Settlement Administrator that it is Google's current policy to voluntarily honor such requests, if the Books or Inserts are individually specified, are in copyright, and the author or publisher has a valid and unchallenged copyright interest in their Books and Inserts". Obviously Google here goes beyond implying that such requests are not to be conceived as binding and it can-

---

31. Supplemental notice available at [http://static.googleusercontent.com/external\\_content/untrusted\\_dlcp/www.googlebooksettlement.com/en/us/Supplemental-Notice.pdf](http://static.googleusercontent.com/external_content/untrusted_dlcp/www.googlebooksettlement.com/en/us/Supplemental-Notice.pdf).

32. The opting-out deadline differs from the removal deadline. Removal refers to the demand made by a right holder that his book which has already been digitized be extracted from the Google Library Project. The Removal deadline according to the supplemental notice published by Google was extended from April 5, 2011 to March 9, 2012. (The Removal deadline as to the libraries' digital copies remains April 5, 2011). Supplemental notice available at [http://static.googleusercontent.com/external\\_content/untrusted\\_dlcp/www.googlebooksettlement.com/en/us/Supplemental-Notice.pdf](http://static.googleusercontent.com/external_content/untrusted_dlcp/www.googlebooksettlement.com/en/us/Supplemental-Notice.pdf).

33. <http://www.googlebooksettlement.com/help/bin/answer.py?answer=118704&hl=en#q17>

34. Insert definition as given by Google:

"Content from one source is an «Insert» if it meets all of the following conditions: 1)It must be text; or tables, charts, graphs that are not pictorial works; and,2)It must be contained in a Book, government work or public domain book that was published on or before January 5, 2009; and,3) It must be protected by a U.S. copyright where the U.S. copyright interest in the Insert is held by someone *other than* a Rights holder of the Book's «Principal Work.» (For example, if you own rights in a poem that is contained in a Book for which you also hold a U.S. copyright interest, then your poem, as it appears in your Book, is not an Insert; however, it would be an Insert if the poem is contained in a Book for which someone else holds the U.S. copyright interest); and,4) It must have been registered – either alone or as part of another work – with the U.S. Copyright Office on or before January 5, 2009, UNLESS the Insert or that other work is not a «United States work,» in which case such registration is not required". Available at <http://www.googlebooksettlement.com/help/bin/answer.py?answer=118722&hl=en#insert>.

not be guaranteed that in the future such requests shall remain under consideration. As Judge Chin put it in the conclusion of his decision to deny the settlement “many of the concerns raised in the objections would be ameliorated if the ASA were converted from an opt-out settlement to an opt-in settlement”.

### **The first settlement agreement v. the amended settlement agreement and the intervention of the US DoJo**

Several of the crucial changes made by the amended settlement were:

1) The removal of many foreign rights holders from the settlement class by redefining “book” to include only non-U.S. works registered with the U.S. Copyright Office or published in Canada, Australia, or the United Kingdom on or before January 5, 2009 (ASA §1.19) rather than “any book subject to a U.S copyright interest as of the Notice of Commencement date” as was proposed in the original settlement. Google in response to foreign copyright holders’ disapproval and non-recognition of the opting-out policy as an equivalent to copyright protection, decided, instead of considering an opting-in policy together with foreign participation in the class action representation (as contemplated by the DoJ), to limit the scope of the settlement by redefining its amplitude. The alternatives as presented by the DoJ would probably require an enormous amount of money in the licensing agreements and would be faced with extra difficulties as the willingness of participation in the class action would imply some form of fostering of the Project on a non-US basis, which should not be taken for granted.

For the time being, only foreign authors whose books were published outside the U.S. but are in the collection of a U.S. library, from which they were digitized, can register with the Book Rights Registry and receive compensation; otherwise only holders of U.S. copyrights worldwide can register their works with the Book Rights Registry<sup>35</sup>. Naturally, regardless of the approval or not of the settlement agreement, litigation in foreign jurisdictions is possible and more than highly likely.

2) The removal of the provision granting Google the right to any more favorable terms that the Registry negotiates with third-parties over the next 10 years. The specific provision could clearly be deemed anti-competitive in nature.

3) “To explicitly recognize rights holders’ right to authorize, through the Registry or otherwise, any third party to use their copyrighted content in any way, including ways provided for under this Amended Settlement Agreement (ASA)<sup>36</sup>”. In Article 2.4 of the amended settlement the authorization granted to Google under the

---

35. Question 17 available at <http://books.google.com/googlebooks/agreement/faq.html#q16>.

36. *Id.*

settlement is characterized as non-exclusive. In order to deal with anti- Google allegations speaking of anti-competitive and anti-trust techniques that solely aim at a monopoly over innumerable works, Google expressly notes that “nothing in this amended settlement agreement shall be construed as limiting any Rights holder’s right to authorize, through the Registry or otherwise, any Person, including direct competitors of Google, to use his or her or its Books or Inserts in any way, including ways identical to those provided for under this Amended Settlement Agreement (ASA)<sup>37</sup>”.

4) “To appoint an independent fiduciary to represent rights holders who have not claimed their works and authorize the fiduciary to spend part of the revenue derived from unclaimed works in searching for their rights holders<sup>38</sup>”.

5) “To extend the date for rights holders to request “removal” of their works from the books database to April 5, 2011<sup>39</sup>”, which was subsequently extended to March 9, 2012.

6) “To allow rights holders to direct the Registry to make their books available at no charge, pursuant to one of several standard licenses (e.g., Creative Commons licenses) or similar contractual permissions for use authorized by the Registry<sup>40</sup>”. Users in general will be able (as understood after the clarifications made by the amended settlement) to access the digital content in several different ways either through purchase of access or under some circumstances for free. Such ways include: preview (free preview of a limited number of pages automatic upon out-of-print works, upon approval of the right holder for in-print books), consumer purchase (for entire books), institutional subscription (for academic, corporate, and government organizations), free public library access (free, full-text, online viewing of in-copyright, out-of-print books at designated computers in U.S) and future services including Print-On –Demand and Consumer Subscription<sup>41</sup>.

7) “To allow the Registry, in its discretion, to authorize more than one free terminals per public library.”

---

37. Article 2.4 of the ASA.

38. Kate m. Manuel, the google library project: is digitization for purposes of online indexing fair use under copyright law?, At 14, cong. Res. Service (nov. 27, 2009).

39. Id.

40. Id.

41. <http://books.google.com/googlebooks/agreement/faq.html>.

- 8) To specify that Google will not provide personally identifiable information about users to the Registry “other than as required by law or valid legal process<sup>42</sup>”.

The amended settlement, amongst the Project’s opponents or those who remain in doubt, could be seen as ineffective in that it still “gives Google and/or the Registry effective control over orphan works; could have anticompetitive effects; fails to protect users’ privacy; and does not adequately promote fundamental library values<sup>43</sup>”. However, Google’s efforts to find a solution that will meet with the demands of right holders and overrule the skepticism generated by its initial, -in other words, financial- objectives cannot be left without recognition.

#### **4) Legal repercussions**

##### ***A) Copyright Liability-three target points***

- i) The creation of intermediate copies/Digitization of full text into the Google search Database
- ii) Partial availability of scanned and stored works by user request- the so called “snippets”
- iii) The distribution provision regarding the partner libraries- the digital library copy

##### ***B) The fair use defense and the four factor test***

Google based her defense against the rights holders’ allegations of copyright infringement on the fact that even if found to be infringing, the Library Project constituted a fair use. According to 17 U.S.C §107 “the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright” even if these actions are therefore made without the rights holders’ consent. The criteria for the determination of fair use include (thus are not limited to): i) the purpose/character of the use, ii) the nature of the copyrighted work, iii) the amount and substantiality of the portion used, iv) the effect of the use on the market.

---

42. Kate m. Manuel, the google library project: is digitization for purposes of online indexing fair use under copyright law?, At 14, cong. Res. Service (nov. 27, 2009).

43. Id at 15.

These four factors are not exhaustive and should not be treated in isolation, one from another<sup>44</sup>. Rather, “all are to be explored, and the results weighed together, in light of the purpose of copyright<sup>45</sup>,” which is to promote the progress of science and the useful arts<sup>46</sup> and serve the public welfare<sup>47</sup>. Although a case by case analysis<sup>48</sup> is needed to determine whether the fair use defense applies to every specific case, previous case law might prove to be helpful together with the corresponding findings of fact<sup>49</sup>. Because fair use is an “equitable rule of reason” to be applied in light of copyright law’s overall purposes, other relevant factors may be considered<sup>50</sup>.

## I) The purpose/character of the use

### a) *Kelly v. Arriba*

Regarding the purpose and character of the use, there are two parameters to be considered: whether or not the use is commercial and whether or not the use is transformative. The main case used by Google to support its position would be *Kelly v. Arriba Soft*. In this case, Kelly who was a professional photographer brought a claim against Arriba Soft which was an internet search engine that displayed low-quality thumbnails of pictures it had copied from other locations on the web. Arriba created a computer program that would search the web for images to index, then download them into its server, generate lower resolution thumbnails and then delete the original photocopy. By clicking on the thumbnail the user was redirect to the original internet site where the content was found.

The court decided in this case that even when a use is deemed to be commercial the “transformative use” factor might still prevail in favor of fair use. Arriba’s use of the thumbnails was therefore found to be transformative. “The Supreme Court has rejected the proposition that a commercial use of the copyrighted material ends the inquiry under this factor instead, the central purpose of this investigation is to see whether the new work merely supersedes the objects of the original creation, or instead adds something new, with a further purpose or different

---

44. *Campell v. Acuff-Rose Music Inc.*, 510 U.S.569, 578 (1994).

45. Id. Kate m. Manuel, the google library project:is digitization for purposes of online indexing fair use under copyright law?, At 14,cong.Res.Service(nov. 27,2009).

46. U.S. CONST, art. I, §8, CL.

47. *Perfect 10, Inc. v.Amazon.com, Inc.*, 487 F.3d 701,720 (9<sup>th</sup> Circ.2007).

48. *Campell*,510 U.S. at 577-78.

49. Kate m. Manuel, the google library project: is digitization for purposes of online indexing fair use under copyright law?, At 14,cong.Res. Service (nov. 27, 2009).

50. *Steward v. Abend*, 495 U.S.207, 237 (1990).



character, altering the first with new expression, meaning, or message; it asks, in other words, whether and to what extent the new work is transformative<sup>51</sup>. Although Kelly supported that mere transformation in another medium has been deemed insufficient to comply with the transformative criteria, the court suggested that since the resulting use of the copyrighted work was not the same with the original use and Arriba's use did not supersede Kelly use, this was irrelevant.

Google based on the *Kelly v Arriba* case, underlines that although it is making a commercial use<sup>52</sup> and it is altering books into a different, digital medium, its use is transformative and thus fair use. Firstly, although the project is operated for commercial reasons, it will not profit from the sale of copies of the book and in that sense its use of the books is not highly exploitative. Google suggests that the GLP will not eliminate the need for the original books but rather augment access to them by creating the index and displaying only a few snippets of the original work<sup>53</sup>. Indexing can be considered a transformative use in analogy to the Arriba case very easily. As the original photographs were intended "to inform and to engage the viewer in an aesthetic experience," Arriba's indexing served a completely different function "improving access to information on the internet<sup>54</sup>". In the same way, snippets of books do not serve the same purpose as reading the book and the digital index merely facilitates access to them.

#### b) *Perfect 10 v. Amazon*

Another interesting case issued by the 9<sup>th</sup> Circuit in 2007, which could be used in favor of Google, would be *Perfect 10, Inc. v. Amazon.com*<sup>55</sup>. "Perfect 10 published erotic photographs in a magazine and a website and claimed that Google. Inc

51. *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 579, 114 S. Ct. 1164, 127 L.Ed.2d 500 (1994).

52. About advertising shown with the books in the project, Google in its website states that: "As with advertising currently offered through Google's Partner Program, advertising may be displayed on books.google.com web-pages. Advertising will not be overlaid on pages from a book. Rights holders will receive the majority of the revenue from the advertising on web pages for specific books. As with all revenues paid by Google to rights holders, if the rights holder cannot be found immediately, the Book Rights Registry will hold the advertising revenue for a reasonable period of time for the rights holder to claim".

53. Jonathan Band, The Google Library Project: both sides of the story, at 4 (2006), *Plagiarism: Cross-Disciplinary Studies in Plagiarism, Fabrication, and Falsification*, 1 (2): 1-17. See also Bottis M., Google Library Project and copyrights of publishers and authors, *τεκμήριον*, 2007, 7, pp. 175-188.

54. 336 F.3d 811 (9<sup>th</sup> Cir.2003) at 818-819.

55. *Perfect 10, Inc. v. Google, Inc.*, 416 F. Supp. 2d 828, 831-32 (C.D. Cal. 2006), aff'd in part, rev'd in part, 487 F.3d 701 (9<sup>th</sup> Cir. 2007).

infringed its copyright firstly by displaying thumbnails of its images in its search results and secondly by directing to third-party infringing websites that actually contained full size images of Perfect 10. In fact, Google scanned and stored photos from the infringing websites in its database, displayed thumbnails of them in response to search queries, and provided links to the third-party sites. The plaintiffs sought to differentiate their case to the *Kelly v. Arriba* one in two ways. The first one was by stating that some of the sites containing infringing images participated in Google's AdSense program despite the fact that Google didn't normally have advertisements on image search result pages, and the second one was by asserting that Google by presenting the thumbnails undermined Perfect 10's market for cell-phone thumbnails, as the company had an agreement to license the specific thumbnails to a cell-phone company called Fonestarz.

The United States Court of Appeals for the Ninth Circuit reversed the district court's rejection of Google's fair use defense and reaffirmed its holding in *Arriba Soft*. The Ninth Circuit found that there was no evidence that the Google thumbnails superseded the Fonestarz cell-phone downloads and ruled that "the transformative nature of Google's use is more significant than any incidental superseding use or minor commercial aspect of Google's search engine and web site". To be exact, Google's thumbnail use was deemed "highly transformative." In fact, the court went so far as to say that "a search engine may be more transformative than a parody," it represents the quintessential fair use, "because a search engine provides an entirely new use for the original work, while a parody typically has the same entertainment purpose as the original work.»

Fair use flexibly during a period of unending technological evolution as well as the relation between "transformative use" and social benefit are factors that could prove to be determinative if taken into account in the GLP case. Google could build a strong defense based on its contribution to preserve the global books reserve through digital access. In *Perfect 10* the court noted that "a search engine provides social benefit by incorporating an original work into a new work, namely, an electronic reference tool<sup>56</sup>". Taking into account the amount of original works incorporated into the digital library as well as the intellectual and educational advantages provided by the accessibility of this content, Google should probably win the public benefit argument. The project would undeniably benefit both authors and publishers in terms of income streams by creating new audiences as well as people with disabilities who would be able to access books converted into Braille and audio formats and all sorts of individuals, research institutions, libraries etc who will be helped to gain access to rare materials otherwise unapproachable. However as Judge Chin mentioned in his decision on the GLP

---

56. *Perfect 10 Inc.*, 487 F.3d at 721.

“while the digitization of books and the creation of a universal digital library would benefit many, the Amended Settlement Agreement (ASA) would simply go too far”.

*c) Sony Corporation of America v. Universal City Studios case*

In *Sony*, the Court held that the sale of the video recording machine, which was used to “time shift” broadcast television for personal home viewing, was not contributory copyright infringement. Stating the *Sega* case<sup>57</sup>, the Court found that intermediate copying, when necessary to gain access to the functional element of the software itself, constituted fair use. Fair use was also based on the fact that the intermediate copies themselves permitted a non-infringing function such as time-shifting. In analogy to the *Sony* case, Google could state that its digitization, as a process of intermediate copying, is incidental and necessary in order to guarantee access to books. Then Google would be left to prove that the presentation of the snippets doesn’t constitute copyright infringement either. “The analogy to *Sony* might not be enough to persuade a court that digitizing for purposes of non infringing indexing constitutes a fair use, however. Digitizing and indexing print books are arguably far removed from making and selling devices that consumers use to record broadcast television programming and replay it later. Additionally, courts have shown little inclination to recognize categories of judicially created fair uses other than time shifting<sup>58</sup>”.

*d) UMG v. MR3.com*

On the other side of the spectrum, in *UMG Recordings v. MP3.com, Inc.*<sup>59</sup>, the fair use defense was rejected on the basis that simple “repackaging” to “facilitate transmission through another medium” cannot constitute fair use. In this case, the plaintiff recording companies sued MR.com for permitting via MP3 technology, the conversion of compact disk recordings into internet accessible computer files which would permit subscribers to access the songs from any place simply by using an internet connection. The unauthorized copying of the plaintiffs’ audio CDs, despite enabling CD owners to “space shift”, was found different from the *Sony* case in terms of adding “no new aesthetics, new insight and understandings to the original recordings<sup>60</sup>” but merely retransmitting the same expression into a different medium. The court also noted that “while such services (MP3

57. *Sega Enterprises Ltd. v. Accoladde, Inc.*, 977, 1524-26, F.2d 1510 (9<sup>th</sup> Cir. 1993).

58. Kate m. Manuel, the google library project: is digitization for purposes of online indexing fair use under copyright law?, At 7, cong. Res. Service (nov. 27, 2009).

59. *UMG v. Mp3 Inc.*, 92 F. Supp.2d 349 (S.D.N.Y. 2000).

60. *Id* at 351.

technology) may be innovative, they are not transformative<sup>61</sup>”; therefore undermining the public benefit theory as supported in the Perfect 10 case.

### **The nature of the copyrighted work**

Under this criterion, the Court examines whether a copyrighted work is factual or creative, granting a greater deal of protection to creative works. However, because within the realms of the project billions of books of both categories will be digitized it is hard to say whether the factor will count against Google or if the court will graciously disregard it, focusing its attention on the other three factors as being more critical to establish a conclusion. It's also possible that some “materials may be nonfiction and mix unprotected ideas with protected expressions of these ideas<sup>62</sup>” making calculations even more complicated. “This diversity of materials makes possible the arguments of both proponents and opponents of the view that projects like Google Book Search constitute fair uses. The nature of the work can, however, be less important than the purpose and character of the use, at least in situations where the use can be clearly recognized as transformative<sup>63</sup>”.

### **The amount and substantiality of the portion used**

This is one more factor that could weight either for or against Google depending on the case law the court decides to endorse. In general, “while wholesale copying does not preclude fair use *per se*, copying an entire work militates against a finding of fair use<sup>64</sup>” and Google will undeniably have to proceed in full-text copying in order to realize the project. If the court follows the decision in UMG v. MR3 it will have to deny the fair use claim. If it follows the Kelly v. Arriba case however, it will be called to take into account whether copying the entire works is reasonable given the purpose and character of the use. “The question would thus become whether such wholesale copying was reasonable for an indexing project<sup>65</sup>” and the Court would either favor Google, as it is impossible to index and present snippets without having digitized the entire book, or decide “that this factor is neutral weighing neither for nor against a finding of fair use because

---

61. Id.

62. Id.

63. Congressional Research service/The Google library project: Is digitization for purposes of online indexing fair use under Copyright law? By Kate M.Manuel, November 27,2009.

64. *Worldwide Church of God v. Philadelphia Church of God,Inc.*, 227 F.3d 110, 1118 (9<sup>th</sup> Cir. 2000).

65. Kate m. Manuel, the google library project:is digitization for purposes of online indexing fair use under copyright law?, Cong.Res.Service (nov. 27, 2009).

the secondary use necessitates use of the entire copyrighted work<sup>66</sup>. Opponents, in contrast, could argue that, “in all cases where courts protected wholesale copying for purposes of indexing, the authors had placed their works online, thereby creating implied licenses for others to copy and index them. Moreover, in at least some of these cases, the copies were deleted after the indexing was completed. In no case did the copier propose to give copies to third parties, as Google did when contracting to provide digital copies of the books in their collections to libraries<sup>67</sup>”.

### **The effect of use on the market**

“The outcome of any findings by the court on this factor may hinge upon the degree of harm to their markets that plaintiffs must show<sup>68</sup>”. The courts have been known to make a distinction between the markets “likely to be developed (potential markets)” and established markets (immediate markets), in terms of proof of actual losses. “The fact that a use is transformative can, however, outweigh even inhibition of or harm to plaintiffs’ markets<sup>69</sup>”. “Whereas a work that merely supplants or supersedes another is likely to cause a substantially adverse impact on the potential market of the original, a transformative work is less likely to do so<sup>70</sup>”. On the other hand, according to the decision in *UMG v. MR3.com* “any alleged positive impact of defendant’s activities on plaintiff’s prior market in no way frees the defendant to usurp a further market that directly derives from reproduction of the plaintiff’s copyrighted works<sup>71</sup>”.

Another factor considered by the courts in their decision in *Field v. Google Inc*<sup>72</sup> was whether the alleged infringer has acted in good faith<sup>73</sup> which could be in favor of Google taking into consideration its presentation of only snippets, its general efforts to find a solution to which both sides agree and its willingness to upgrade any book into the revenue sharing Partner Program<sup>74</sup>. From a realistic point of view and regardless of whether the plaintiffs will be able to show that

---

66. Emily anne proskine, *googles technicolor dreamcoat: a copyright analysis of the google book search library project*, at 8,21 berkeley tech.L.J.213.

67. *Id.*

68. *Id.*

69. *Id.*

70. *Acuff-Rose*, 510 U.S.,590,591.

71. *UMG v. Mp3 Inc.*, 92 F. Supp.2d 349,352 (S.D.N.Y.2000).

72. 412 F.Supp.2d 1106 (D.Nev.2006).

73. *Id.* at 1122.

74. Jonathan band, *the long winding road to th google books settlement*,fn.160,9 J. Marshall rev. Intell.Prop. L. 227.

the Project could be harmful to the market of books (which is unlikely considering the disappointing percentages<sup>75</sup> of book usage for purposes other than research), a digital library serving as a liaison to bookstores and libraries around the world can only be seen as a promising evolution to the book market. Let's not forget that the expedited rhythms of internet-orientation are quickly serving as a substitute for many recreational activities, especially among the new generations making the percentages of young people reading books smaller every year. This specific target group will turn to the internet to acquire the information it seeks to absorb and a digital market for books might be the only effective way to approach it.

### International dimensions

Roughly 50% of the books digitized by the Google Library Project will be in languages other than English, with more than 100 languages represented<sup>76</sup>. U.S. consumers will be enabled to buy online access to millions of books by European authors whose works are scanned in US Libraries. However concerns regarding the digitization are reaching the level of strong opposition both in Europe and elsewhere. As the president of France, Nicolas Sarkozy characteristically said on December 8, 2009 speaking about the Project, "France is not going to be stripped of what generations and generations have produced in the French language, just because it isn't capable of funding its own digitization project<sup>77, 78</sup>". Many more European countries (such as Germany<sup>79</sup>, Austria, Switzerland, Spain etc) as well

---

75. Statistics available at [http://www.publishers.org/main/IndustryStats/indStats\\_02.htm](http://www.publishers.org/main/IndustryStats/indStats_02.htm), "Book sales fell 1.8% in 2009. This followed a larger drop of 2.6% in 2008. From these numbers, we can see the overall effect of the Great Recession on book sales", "Books are no longer counter-cyclical and no longer recession-proof" available at <http://www.examiner.com/x-25786-SF-Publishing-Examiner~y2010m4d11-New-book-sales-statistics-released-for-last-year>.

76. <http://www.eff.org/deeplinks/2009/08/google-book-search-settlement-access>.

77. The European Union has launched a "parallel" project in view of the need to create digitized resources for consumers and the need to become more competitive such as the Europeana Project. However concerns about orphan works do not cease to create questions in Europe as well, especially taking into consideration the moral right regime which generates advanced protection for the author of creative material. See <http://europeana.eu/portal/>.

78. Bruce Crumley, *Europe v. Google: the next chapter*, available at <http://www.time.com/time/world/article/0,8599,1946920,00.html>.

79. In Germany 2700 people have signed a petition asking the Government to try to stop Google. See Kevin J. O'Brien and ERIC Pfanner, *European opposition grows to Google's digital books plan. Publishers and authors are divided on whether online sales are a threat*, International Herald Tribune available at <http://www.highbeam.com/doc/1P1-169772768.html>.

as non-European countries such as China, are in the same spirit as France<sup>80</sup> regarding the GLP.

Google faced a lawsuit in France by a publishing company called “La Martiniere Groupe” joined by the French Publishers Association (FPA), which accused Google of infringing its copyright by scanning books whose copyright it owned. On December 18, 2009, Google’s book search project suffered a legal setback in Paris, as the court ordered it to pay €300,000 (US\$432,000) in damages for breach of copyright, and called it to stop distributing digital copies of French books to French Internet users without the permission of their publishers<sup>81</sup>. Despite the fact that the amount is not that significant considering Google’s gigantic amount of revenues, the case is symbolic of the intentions of Europe.

Britain, known for its close relationship to the U.S, has not forcefully reacted to the Project or settlement and instead is expressing concerns regarding practical issues such as the determination of whether a book is out-of-print if it is not available in the States but is widely available in Europe<sup>82</sup>. Britain is also the only European Country participating in the Books Registry together with Australia and Canada (books published in Great Britain fit the definition of “book” as given by the amended settlement), which although could be explained based on the principal linguistic similarities of the above countries, is not enough to justify the lack of adequate European representation in a Project that would influence Europe as intensely as this.

Even the European Commission looked into the project by summoning a hearing on August 3, 2009, regarding possible effects of the project on European intellectual property rights. In the hearing, Google’s representative was present to reassure the European critics that: a) foreign authors and publishers would be allowed to appoint two representatives to the board of the Books Rights Registry, b) it would only display out-of-print translations of works that were still commercially available in Europe with the approval of their copyright holders, c) greater efforts would be made to ensure that books are truly out-of-print before

---

80. Id.

81. Peter Sayer, Paris Court Rules Against Google in Book Copyright Case(Dec.18,2009), available at [http://www.pcworld.com/businesscenter/article/185092/paris\\_court\\_rules\\_against\\_google\\_in\\_book\\_copyright\\_case.html](http://www.pcworld.com/businesscenter/article/185092/paris_court_rules_against_google_in_book_copyright_case.html).

82. Kevin J. O’ Brien and ERIC Pfanner, European opposition grows to Google’s digital books plan. Publishers and authors are divided on whether online sales are a threat, International Herald Tribune (Aug.24,2009),available at <http://www.highbeam.com/doc/1P1-169772768.html>.

making them available in digital form<sup>83</sup>. The Commission was concerned with accusations against Google again on February 24, 2010, when it confirmed it had received 3 complaints from three internet companies accusing Google of anti-competitive behavior by lowering their search rankings.

The basic objections coming from foreign rights holders have to do with a) the inadequacy of the class notice and class representation b) the orphan works issue<sup>84</sup> and c) international law concerns that refer to the opting out policy which would require them to determine whether they are covered by the settlement and to decide to opt-out instead of opting in. The Berne Convention and the agreement on the trade related aspects of IP rights could in no way be read as allowing such a project without a simultaneous violation of international law at its core. Other concerns include fears of prejudicial treatment of certain rights holders (UK, Canada, and Australia) by favoring their counterparts of certain nations in terms of copyright protection. Google has responded to international law concerns by saying that "this case is about United States copyright interests. It's about uses of works in the United States<sup>85</sup>". Google's answer shows an utter disregard of foreign rights making us wonder whether Google itself has no realization of the dimensions of its own project or if it simply pretends not to.

## Conclusion

Global harmonization has to be achieved through the conception of a golden rule between respect of international intellectual property regimes and the US system, as to allow everyone to draw the innumerable benefits arising from Google's initiative to create an online library. Since the project is ambitious enough to incorporate books arriving from the four corners of the planet, a greater deal of respect should be afforded to right holders whose works are suddenly and without their permission in the center of digital renovation.

The fair use doctrine however, might need to be reformed in order to affectively apply to potential infringement cases coming from the benign of internet use proliferation. As underlined in the Amended Settlement Agreement (ASA) rejection,

---

83. See Google gives ground at EU hearing available at <http://www.spiegel.de/international/europe/0,1518,647700,00.html>.

84. Germany with her written intervention before the court stated that: "Competing digital libraries in Germany (Deutsche Digitale Bibliothek) and throughout the world do not enjoy rights to such authors or "orphan works" because Germany requires licensing of rights prior to the usage of orphan works. Such a sweeping de facto compulsory license system would require legislative action (equivalent to Congressional action) in Germany".

85. Hr'g Tr. 157-58 (Daralyn J. Durie).



there are many questions deriving from the GLP which are “better left for Congress” and maybe Google’s project can be seen as a scapegoat, opening the road for updated legislation dealing with all those copyright issues that Congress has been avoiding to legislate for some time now. Between the theories that could potentially be adopted is: 1) the replacement of the right of reproduction, in other words the right of making copies, with a boldly canvassed (and restrained in its scope) right to control public distribution of a copyrighted work<sup>86</sup> or 2) the adoption of a different set of criteria with regard to the application of the fair use doctrine online. At any case, paranoid, bellicose obsessions against the so-called “googlization” phenomenon have no chances of leading to innovation.

---

86. Ernest Miller and joan feigenbaum, taking the copy out of copyright, available at <http://cs-www.Cs.Yale.Edu/homes/jf/mf.Pdf>.

# **Electronic government: its course in United States, European Union & Greece**

---

---

**Aikaterini Yiannoukakou**

---

---

## **1. Introduction**

The term “electronic government” has been introduced to the scientific field during the last 10 – 15 years determining the transformation of the public administration by using the ICTs (Information & Communication Technologies). However, this concept has been under discussion for at least the middle of the 1980s to the early debates on how public administration could be more effective, to the point and reduce the duplicate tasks performed by organizations of similar or relative function. It is common knowledge that public organisations generate vast amounts of information that need to be edited, saved, manipulated and stored somehow. The use of IT is the most efficient method to manipulate and control the usability of these enormous amounts of produced information faster and more flexible than with manual manipulation such as paper files, forms, handbook etc. (Milward, and Snyder, 1996, p. 261).

Nevertheless, we must not confuse the automation of the traditional paper-based bureaucratic administration into electronic format by using computers and telecommunications technologies. Instead, the core of e-government is about re-engineering of operations and transforming the entire working mentality of public administration’s back office by adopting ICTs. The main target is to increase the efficiency and effectiveness of public administration, to reduce the costs and to supply a more qualitative and straight-forward services.

Most experts agree upon that it is almost unattainable to provide a single definition for e-government due to the complex nature of the phenomenon, as it is a multidimensional concept with many inter-dependable aspects relying on political, technological, economical, social, administrative and legal issues. Thus, most researchers provide with a definition that applies on their point of view. However in respect to consistency, we will try to give a simple definition to “e-government” as “a way for governments to use the most innovative ICTs, particularly web-based Internet applications, to provide citizens and businesses with more convenient access to government information and services, to improve the quality of the services and to provide greater opportunities to participate in democratic institutions and process” (Fang, 2002, p. 1).

As mentioned above, the core issue to e-government discussions focuses on that it is not related with technology itself. On the contrary, it referees to the re-organisation of public administration by using technology. The vision of e-government can be summarised as following:

1. Seamless online access to governmental services 24/7 (24 hours a day – 7 days a week) abrogating the barrier of access to a preset period of time with physical presence to the agencies, namely the hours that the agencies are open to the public.
2. Adoption of a horizontal agency-independent and customer-centered model of administration, as citizens do not care about the number of agencies needed to conclude a task –i.e issuing a driving license– but merely they are interested in getting their job done fast and almost “painless”.
3. Reduction of both transaction costs and the governmental expenses. This is about to happen by eliminating the redundant and/or duplicated procedures with better online control.
4. Amplification of the social capital and the reversal of the public opinion regarding the capability of the government to solve social problems. This could be done from one hand by providing simple procedures as issuing a birth certificate in paperless and queue-free environment, and by the other hand by establishing a more open and direct communication with the citizens and aiming to their active participation.

However, for all these to happen the first necessary step is the development of a national policy that will clearly describe the intentions of each government and will lay out long-term measures in order to implement successfully e-government. This policy must not focus on specific applications or services, but mainly should provide the means through which specific applications should be developed. Also, all this effort must be accompanied by a legislative and regulatory framework, which will specify all the pending issues regarding data privacy, systems security, the technology used, the political, economical and ethical implications imposed by the transfer from the paper-based to electronic public administration.

To this article I point out the efforts of United States, European Union and Greece have taken in the legislative and regulatory field in order to develop a national policy regarding the implementation of e-government. I refer to the predominant legislation that imposed the most radical changes to the way public services conducted business.

## 2. United States

United States has rushed into adopting e-government with great enthusiasm in all levels of government –federal, state and local– either by doing the obvious and creating governmental sites or by issuing national policies and regulations. To the early studies, United States were considered as a role model for e-government, mainly due to the penetration rate in Internet usage and because they had developed innovative e-commerce applications in comparison with other countries (Hagen, 2004).

United States present a unique administrative format, which consists of “...a horizontal separation of powers between the legislative, executive and judiciary, and by a vertical separation between the federal, state and local government” (Hagen, 2004, p. 211). However, the independence between federal and state government is ensured by American Constitution, whereas the local –and further more the tribal–governments are mostly regulated by the states’ legislation. In the scope of this horizontal separation, the federal government traditionally holds reduced powers limited to foreign politics, defense and interstate commerce, whilst all other powers have been assigned to the individual states without sharing powers with each other. However as the political and administrative system progressed, the legislative powers of federal government had been extended to include social welfare policy and infrastructure, such as transportation, education and regional planning (Hagen, 2004). The legislation on e-government falls under the concept of national infrastructure.

The government of United States is the biggest producer of government information worldwide, which has to be controlled, checked, stored and be available in every instance. As a result, there is a complex –almost chaotic– administrative structure between all levels of government, each of which maintains its independency regardless if they commonly cooperate to carry out specific programs. For that reason, public administration in US has been using the advances in IT for a long time replacing the paper-based system with an automated one, beginning from the use of mainframes and video-text based systems to public websites and intranets. Since the early 1990s, US has been a pioneer in introducing IT applications into the administrative processes of the government, sometimes successfully and others somewhat a fluff, but always trying to increase the productivity of the public sector, and hence the economic competitiveness and growth.

### *National performance review (1993)*

the first serious and organised attempt to create a national policy on e-government begun when President Bill Clinton and Vice-President Al Gore got elected to the

White House in 1993. Then Vice-President Gore realised that the most important task in order to improve the services of public administration was to develop a national policy on how to take advantage of IT developments that would take US to the next level. So in September 1993, the report "From Red Tape to Results: Creating a Government that Works Better and Cost Less" was published in cooperation with the National Performance Review (NPR), an interagency task force created especially to study the government's administrative reformation. In the six month period prior to the completion of the report, the task force and Al Gore himself participated to several meetings with agencies, committees and public officials in their effort to ascertain the administrative and bureaucratic problems faced by the employees. Based on the experience gained from these meetings, VP Gore decided to focus on how the government really works, instead of the ideal "what should be doing", and make recommendations that would alter the practicality and daily interaction both of the employees and the citizens. As stated by him the main objective was "to create a government that works better and cost less by empowering employees to put customers first, cutting the red tape that holds back employees and cutting back to basis" (National Performance Review, 1993a).

The main measures to achieve the main objective were (Hagen, 2004, p. 217):

- Reduction of the budget process
- Decentralisation of human resources management
- Reduction of the procurement system
- Modification of the Inspector General's responsibilities
- Abolition of unnecessary administrative regulations
- Strengthening of the States' governments and the local authorities and make them more flexible.

The report was immediately supported by President Clinton, and was finally accompanied by 38 supplementary reports, among which was the "Re-engineering through Information Technology", a report that emphasized the importance of the deployment of IT in the reform effort and placed it among the top priorities of the new government. The report consisted of three (3) parts aiming to better spread IT benefits to government (National Performance Review, 1993b):

1. Strengthen Leadership in Information Technology: the Information Infrastructure Task Force (IITF) was positioned as a leader with a dual cause (a) to plan strategically the telecommunications and computer technology implementation to public administration, and (b) to develop the National Information Infrastructure.

2. Implementing Electronic Government: the report proposed seven (7) initiatives that would move government from paper-based to electronic era, and fundamentally alter the communication between agencies and citizens, whilst at the same time would provide substantial return on investment through increased productivity.
3. Establishing Support Mechanism for Electronic Government: the federal government in cooperation with the private sector would processed to the development of a National Information Infrastructure (NII) in order to “... revolutionize the way we work, learn, shop, and live, and will provide Americans the information they need, when they need it, and where they need it –whether in the form of text, images, sound, or video”. Some of the drastic measures proposed in this part of the report can be summarised to the modernization of data processing centers and standardization of government’s administrative functions, the reinvestment of the savings from IT implementation and the creation of a government-wide venture capital fund to finance IT projects within agencies, the adoption of a national protection policy as well as of digital signatures and encryption standards, the introduction of innovative purchasing methods of IT products to obtain state-of-art equipment, and the training and technical assistance to federal employees regarding the new online systems.

### ***Government performance & results act (1993)***

the January of 1993 American Congress passed the Government Performance & Results Act (GPRA) that aimed to “*provide for the establishment of strategic planning and performance measurement in the Federal Government, and for other purposes*” (U.S Office of Management and Budget, 1993), which was finally signed by President Clinton in 3 August 1993. The GPRA introduced a new method of output-oriented budgeting and controlling by instructing agencies to prepare a multi-year strategic plans including IT investments.

The primary purposes were (Radin, 1998, p. 309):

1. To improve the confidence of the people in the capability of the Government by holding federal agencies accountable for achieving program results.
2. To stimulate reform with a series of pilot projects that could be used as examples for others.
3. To promote a focus on results, service quality, and customer satisfaction.
4. To help managers improve service delivery, by requiring them to plan for meeting program objectives and by providing them with information about program results and service quality.

5. To improve congressional decision-making by providing information on achieving statutory objectives and relative effectiveness of various programs, and.
6. To improve internal management of the federal government.

In short, GPRA took management models used in the private sector and incorporated them into the managerial tactics of federal agencies by introducing three (3) main set of requirements, namely the submission of strategic plans covering a 5 years period, the submission of annual performance plans and, finally, the submission of annual performance reports. (U.S Office of Management and Budget, 1993):

However, regardless the positive acceptance of the GPRA, most studies indicate that the actual results were not the desirable due to a number of reasons with most prominent firstly the imposition of a unified cost control mechanism to different types of institutions, where the history has repeatedly denoted that there is no “one size fits all” solution. Secondly, the entire concept of GPRA was drew on experiences from countries with parliamentary tradition such as Australia, New Zealand and UK, which is not applicable to the U.S. system, where there is a horizontal delineation of authorities and vertical sharing of power between federal, state and local governments. As a result, there isn't a national institute with authority to allocate resources and control the budgeting of all levels of the government. Thirdly, GPRA's adoption was based on assumptions regarding the gathering, control and evaluation of agencies' data, which was proven to be much more difficult than expected (Radin, 2000).

### ***Government paperwork elimination act (1998)***

in October 1998, the Congress signed the Government Paperwork Elimination Act (GPEA), which made possible for citizens to exchange information with the federal agencies in full electronic format and at the same time took provision for the application of electronic signatures. Typically, the GPEA enacted the introduction of US into the e-government era as it specifically noted that by 2003 all agencies should provide full electronic access to their information along with online forms submission and electronic filing as an alternative to the paper-based transactions which would be continued to exist for those who wanted to use that format. In short, GPEA provided the following (U.S. Chief Information Officers Council, 1998):

1. Authority to Office of Management & Budget (OMB) to provide for acquisition and use of alternative information technologies, making possible to use IT for the electronic submission, maintenance or disclosure of information as a substitute for the paper and for the use and acceptance of electronic signatures (SEC. 1702).

2. Procedures for use and acceptance of electronic signatures, where within 18 months the OMB in consultation with the National Telecommunications & Information Administration would provide requirements for compatible, standardised, non proprietary and reliable use of electronic signatures (SEC. 1703).
3. Deadline for implementation of procedures for use and acceptance of electronic signatures, where no later than five (5) years by the enactment of the Act the provision under consideration should be implemented in full scale (SEC. 1704).
4. Electronic storage and filing of employment forms, where no later than 18 months by the enactment of the Act procedures to permit private employers to store and file electronically with agencies forms should be developed (SEC. 1705).
5. Study on use of electronic signatures, where OMB in cooperation with the National Telecommunications & Information Administration should conduct an ongoing study on paperwork reduction, individual privacy and security and authenticity of transaction, the results of which should be submitted to the Congress on periodical basis (SEC. 1706).
6. Enforceability and legal effect of electronic records, where the legal effect, validity or enforceability of electronic records created under the provisions of this Act are validated (SEC. 1707).
7. Disclosure of information, where the information collected in electronic format should be used or disclosed for purposes of government practice, or with the prior affirmative consent of the person that the information pertains (SEC. 1708).

Moreover, on May 2000 OMB issued a Memorandum (M-00-01) aiming to provide a guidance to the agencies for successful implementation of GPEA. Further, the OMB charged five (5) federal agencies with developing supplemental GPEA guidance on legal, technical, policy and records management issues. Finally, to complement GPEA electronic signatures requirements the Electronic Signatures in Global & National Commerce Law –the e-Sign Law– was signed by President Clinton in 2000, which stipulated the interchangeability among paper and electronic forms in doing business giving the opportunity to the citizens to decide which version of government want to deal with, the electronic or the paper-based one (Fletcher, 2002).



### ***E-government act (2002)***

in November 2000, George W. Bush won the presidential elections against Al Gore, and, thus, the White House changed hands, and as it has been estimated more than 3.000 employees were exchanged with the new presidency. However, the new leadership pledged to the continuation of its predecessor (Hagen, 2004). Under this scope, the US Congress signed the E-Government Act 2002 (E-GA) in 27<sup>th</sup> of December 2002, a document 72 pages long, in which there is a detailed description of what the e-government should be and how should be implemented to federal government. Namely, the E-GA aims to *“to enhance the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer within the Office of Management & Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes”* (U.S. Congress, 2002).

Basically, the E-GA formed the first integrated legislative effort to effectively manage the IT practices government-wide and to make government information and services available online in a unified manner aiming to greater efficiency, reduce redundancies, achieve intergovernmental coordination and align IT investments (Seifert, 2008).

The E-GA was divided in five (5) Titles which contained the major issues concerning a holistic approach to the implementation of e-government in management, funding, promotion of services, access, use and preservation of information, privacy and security. More specifically, the main points introduced by E-GA were:

1. The establishment of the Office of Electronic Government (OEG) within the OMB, headed by an Administrator –or Federal CIO as is commonly being referred to– appointed directly by the President, with responsibility to improve the delivery of electronic services and increase the inter-governmental cooperation (Title I).
2. The establishment of E-Government Fund within the US Treasury and administrated by the Administrator of the General Services Administration (GSA), which would enable the financing of IT projects related to government electronic services (Title II). As stated, the fund assigned for the fiscal years 2003-2006 reached the total sum of \$345 million dollars, an amount scaled up by far in comparison with the previous years. Unfortunately, and regardless of the intentions of the legislator, the US Congress did not allocate more than \$5 million in any given fiscal year until the FY2006 since the enactment.

3. The enactment of a variety of e-government services and initiatives –such as federal portals, pilot projects, federal courts, geographical information systems, information use, privacy provisions– under detailed description and allocation of responsibilities clarifying that the OMB was the leader and coordinator of all federal e-government services.
4. The enactment of the Federal Information Security Management Act 2002 (Title III), which provided a framework for the information security policies in national scale establishing uniform security standards demanding from the agencies to conduct independent evaluations of their information security programs.
5. The enactment of the Confidential Information Protection & Statistical Efficiency Act 2002 (Title V), which designated the OMB Director the coordination of the confidentiality and disclosure policies, and established limitations on the use and disclosure of data by government agencies.

The E-GA put US dynamically to the chase of an integrated e-government reality and designated it as a leader country in the e-government map worldwide. In November 2007, the E-Government Reauthorization Act 2007 passed, which amended and modernized several sections of E-GA and expanded its activities through the FY2012.

### ***Open government directive***

In November 2008, President Obama was elected and one of his first actions was to sign a Memorandum on the Transparency and Open Government stating his commitment to continue the work of his predecessors regarding e-government. However taking it one step further, he heralded his aim for an open and transparent governance. Quoting his own wording “...my administration is committed to creating an unprecedented level of openness in Government. We will work together to ensure the public trust and establish a system of transparency, public participation, and collaboration. Openness will strengthen our democracy and promote efficiency and effectiveness in Government” (U.S. White House, 2009).

Under this scope the Open Government Directive (M-10-06) was released in 8<sup>th</sup> December 2009 by OMB instructing the Heads of Executive Departments & Agencies to immediately apply the three (3) principles of transparency, participation and collaboration. Transparency refers to making available to the public information of what the Government is doing; and by doing so simultaneously increases Government’s accountability. Participation refers to providing to the public the opportunity to contribute to policy formulation by stating opinions, ideas and feedback on the proposed initiatives. Collaboration refers to establishing systems and methods which ensure a more efficient cooperation across government

levels, and between the public administration and organisations, businesses and individual in the private sector.

Also, the Directive imposes deadlines for the completion of specific actions, which must have be met by following the steps of (a) publishing government information online, (b) improve the quality of government information, (c) create and institutionalise a culture of open government, and (d) create an enabling policy framework for open government. Finally, the Directive requires from the agencies to prepare an open government plan, which would delineate the methods each agency intends to incorporate the 3 principles to its operations, would report specific actions engaged by each agency towards open government and mention specific timeline in achieving them.

### 3. European Union

Since the decade of 1990s, EU has been a leader regarding the formulation of legislative and policy framework on telecommunications, digital tv, computer, data privacy and security issuing legislative and regulatory texts such as the Directive 1999/93/EC, the Directive 2002/22/EC, the Directive 2002/58/EC, the Directive 2006/123/EC. However, EU has delayed –comparing to other developed countries as USA, Australia, Canada, New Zealand– to deploy policies capable to cater to the challenges of the forthcoming e-government. Nevertheless, EU managed by following a stepwise approach to be synchronised with the rest developed countries by adopting the requisite framework through which all Member-States must develop national policies on e-government. For that reason, European Commission along with Council of Europe have periodically published policy frameworks with the distinctive name “**eEurope**” as guidelines in order to move forward to an inclusive, integrated Information Society and level off the differences and disparities among Member-States.

All eEurope initiatives (eEurope, eEurope 2002, eEurope 2005 and i2010) are integral part of the Lisbon Strategy focusing on developing guidelines and generating a framework for the implementation of ICTs and Internet technologies in all aspects of everyday life of Europeans aiming to bring Europe into digital age and accelerate the process towards the implementation of the new economy, an economy based on exploiting the possibilities of information society. As expected, public administration was influenced and, thus, there were special sections devoted on specialised actions regarding the IT reform of public administration and the introduction of e-government both to Member-States’ reality as well as to a pan-european level.

***Europe – an information society for all initiative (1999)***

in December 1999, European Commission put into action the initiative “eEurope–An Information Society for All” that posed ambitious targets in order to bring the benefits of information society to every single European citizen. In order for the goals of information society to be accomplished, the modernisation of European economy should be accelerated and the sectors of employment, growth, productivity and social cohesion should be assisted. The primary objectives of eEurope were (a) to interconnect every citizen, household, school, business and administration by providing to them the possibility of entering digital era, (b) to create an computer literate Europe supporting by a entrepreneurial mentality ready to fund and to develop innovative ideas, and (c) to ensure that the entire process aims to social inclusion (Liinkanen, 2003, p. 70).

For the attainment of these objectives, ten (10) areas of priorities had been set (European Commission, 1999):

1. European youth into the digital age: a three (3) year plan setting an ambitious long-term target that by the end of 2003 all pupils should leave school as “digitally literate”.
2. Cheaper Internet access: Member-States should take measures for the liberalisation of the telecommunication market.
3. Accelerating e-commerce: enactment of a reliable legal framework on the internal market and e-commerce –especially considering the small & medium-sized enterprises (SMEs)– and implementation of electronic procurement to the public domain.
4. Fast Internet for researchers & students: the objective was full access to fastest Internet for all European education and community, thus Internet infrastructures should have been upgraded by the end of 2000, and by the end of 2001 each Member-State must have had at least one university and research center with a network supporting multimedia communications and online interactive lectures, and to make allowances for the expansion to all academic and research institutions of the country.
5. Smart cards for secure electronic access: By the end of 2000, a industry-wide consensus on on common specifications for a generalised smart card infrastructure should have been reach, whereas by the end 2001 smart cards should have been used for secure access to basic payments services, and by the end of 2002 the use should have been extended to sectors as health services and public transportation.

6. Risk capital for high-tech SMEs: The Commission by the end of 2000 should have reviewed the current policy and proposed innovative methods of capital raising, whereas by the end of 2003 the barriers for the formation of a pan-european market on the investments of entrepreneurial funds for the SMEs should be fully removed.
7. eParticipation for the disabled: The Commission should have accelerated the standardisation of accessibility to information and communication services by issuing a relevant recommendation by the end of 2000, while by the end of 2001 all public web sites should have been designed with the provision to be accessible to people with disabilities.
8. Healthcare online: The standardisation of health care informatics to be implemented by the end of 2000, while the health smart card to secure and confidential patient information should have been established by the end of 2003, and by the end of 2004 a telematic health infrastructure for all health professionals and managers should have been installed.
9. Intelligent transport: Enhanced transports with the implementation of the pan-european emergency number 112 with multi-lingual support by the end of 2001, improvement of the traffic informative system throughout Europe, and modernisation of the airborne, ground-based or space-based infrastructures by the end of 2004.
10. Government online: Public information more easily accessible by extending and simplifying Internet access would aim to bring government services closer to the citizen, reduce government expenditure by cutting bureaucracy and red tape, create jobs in value-added services providers, and create better Europe-wide market information.

### ***Eeurope 2002 – an information society for all action plan (2000)***

In continuance the European Commission during the Feira European Council took place in 19-20 June 2000 adopted the Action Plan “eEurope 2002: Information Society for All” as an integral of the Lisbon Strategy 2010. The aim of the Action Plan was to ensure that the targets set during the Lisbon European Council in March 2000 would be accomplished by adopting the necessary measures with deadline for completion the end of 2002.

All actions were clustered around three (3) major objectives (European Commission, 2000):

1. A cheaper, faster secure Internet
2. Investment in people and skills

### 3. Stimulate the use of Internet

More specific for the action “Government Online”, eEurope 2002 required the efforts of public administration in all levels to exploit the advantages of new technologies, so as to make information accessible, where as Member-States were forced to provided generalised electronic access to basic public service by the end of 2003. The Action Plan contained specific actions along with their timeline to be implemented by the EU and the Member-States summarised to the following table (European Commission, 2000):

eEurope2002 Action Plan– Government online – Electronic access to public services		
Action	Actor(s)	Deadline
Essential public data online including legal, administrative cultural, environmental and traffic information	Member-States supported by European Commission	end 2002
Member States to ensure generalised electronic access to main basic public services	Member-States	end 2002/3
Simplified online administrative procedures for business e.g. fast track procedures to set up a company	Member-States, European Commission	end 2002
Develop a co-ordinated approach for public sector information, including at European level	European Commission	end 2000
Promote the use of open source software in the public sector and e-government best practice through exchange of experiences across the Union (through the IST and IDA programmes)	European Commission, Member-States	during 2001
All basic transactions with the European Commission must be available online (e.g. funding, research contracts, recruitment, procurement)	European Commission	end 2001
Promote the use of electronic signatures within the public sector	Member-States, European Institutions	end 2001

Table 1: Government online actions in eEurope2002

The ultimate objective was to remove all constrains hampering the realisation of a pan-european system of public services aiming in increasing efficiency of the

public sector, cut costs of transactions, increase transparency and speed up the implementation of standardised administrative procedures.

### ***eEurope 2005 – an information society for all action plan (2002)***

following the Feira European Council, the Commission prepared the Action Plan “**eEurope 2005: Information Society for All**” to succeed the eEurope 2002 Action Plan. The objective of this Action Plan was “...to provide a favourable environment for private investment and for the creation of new jobs, to boost productivity, to modernise public services, and to give everyone the opportunity to participate in the global information society. eEurope 2005 therefore aims to stimulate secure services, applications and content based on a widely available broadband infrastructure” (European Commission, 2002).

The proposed eEurope 2005 focused firstly on stimulating services, applications and content covering both networked public services and e-business, and secondly addressing the broadband infrastructure by encouraging the widespread availability and use of broadband networks, and moreover the development of Internet protocol IPv6 as well as security matters. Based on those axes, the targets to be met by the end of 2005 were the establishment of online public services (e-government, e-learning services, e-health services) and of a dynamic e-business environment.

Also, eEurope 2005 determined four (4) interrelated components as means of achieving those targets (a) policy measures for the review and the adaptation of legislation both in national and European level ensuring that it did not pose barriers to the development of new services, to strengthen competition and openness, to improve access to a variety of networks, and to demonstrate political leadership, (b) good practices for the facilitation in the exchange of experience and demonstration projects between Member-States, as well as from the notification of lesson from the failures, (c) benchmarking for monitoring and progress evaluation of the projects, thus the progress of accomplishing the objectives, and (d) coordination of existing policies by a steering group supervising the progress of policies and information exchange in national and European level and among all stakeholders.

Especially regarding e-government the proposed actions included:

- Broadband connection to all national public administrations by the end of 2005
- Interoperability on an agreed framework to support pan-european e-government services concerning

- 20 basic public services to be provided interactively, accessible to everyone including people with disabilities, the elders and the minorities by utilising broadband networks and multi-platform access and re-organising the back-offices of public administration of Member-States by the end of 2004
- Member-States should come through with the electronic transaction of a significant part of public procurement by the end of 2005 and EU should customise the legal framework to accommodate this transition
- The establishment of Public Internet Access Points via which access to e-government services should be ensured to all European citizens by specially designed central points in municipalities and communities
- Culture and tourism by defining electronic services for the promotion of Europe and the provision of user-friendly public information.

The Commission having learned by the underachievements of eEurope 2002, in eEurope 2005 Action Plan made the provision for reviewing the actions during their completion as well as conducting an interim review and benchmarking report both presented to the European Council of 2004.

### ***I2010 – an information society for growth and employment (2005)***

In June 2005, European Commission presented the continuance of eEurope 2005, with the title “i2010 – A European Information Society for Growth and Employment”, which aimed to merge the independent initiatives to a uniform and cohesive strategy providing broad policy guidelines for what it is known as “Information Society” to years until 2010.

The i2010 Strategy was the framework through which the primary challenges and developments of Information Society would be addressed until 2010 by focusing on the use of ICTs as driving forces for sustainability, social inclusion and quality of life and laying out three priorities (European Commission, 2005):

- The completion of a Single European Information Space which promoted an open and competitive internal market for information society and media sector
- Strengthening Innovation and Investment in ICT research to promote growth and employment
- Achieving an Inclusive European Information Society which promotes growth and employment in conjunction with sustainable development and prioritises better public services and improved quality of life.

Generally the i2010 Strategy remitted a new integrated policy approach to Information Society contributing to the accomplishment of the Lisbon objective, namely sustainability and employment. Also, Member-States were invited to



adopt National Reform Programs by October 2005 compatible with the three above mentioned priorities underlying the importance of ICT adoption.

Especially concerning e-government, an separate Action Plan was published in April 2006 under the title "i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All" that was based and harmonised with the objectives of i2010 Strategy by soliciting the acceleration of development of electronic public services both in national and in European level, preventing the rise of new constrains on the single market due to fragmentation and lack of interoperability, extending the benefits of e-government across Europe, and ensuring cooperation in designing and delivering e-government services.

Moreover, the i2010 eGovernment Action Plan focused on five (5) primary objectives related to electronic public administration recognising the new challenges arisen by the enlargement of the Union with new Member-States and all the diversities that this elongation entails (Commission of the European Communities, 2006):

1. No citizen left behind by promoting the social inclusion and fighting digital divide through the use of ICTs to public administration so as all citizens would benefit from trusted, accessible and innovative services by the end of 2010.
2. Increasing the efficiency and effectiveness by contributing in achieving increased level of user satisfaction, transparency and accountability, reducing bureaucracy and improving efficiency.
3. Implementation of high-key impact services for citizens and businesses so as by 2010 the totality of public procurement be completed electronically.
4. Putting key enablers in place to provide to citizens and businesses convenient, secure and interoperable authenticated access to public services in European scale by 2010.
5. Enforcement of participation of citizens and empowerment of democratic decision making process by introducing effective public dialogue and participation to democratic decision making by 2010.

The i2010 eGovernment Action Plan designated a detailed description and timeline of individual specific actions for each of the above mentioned objectives, which should be accomplished by the end of 2010 in cooperation of European Commission, the Member-States and stakeholders accompanied by periodic monitoring, evaluation, review and update of the actions.

However, the delay in adopting a legal framework within the EU itself, and, moreover, the delay and the lack of harmonisation on behalf of Member-States in adapting the proposed policies and recommendations to their national law as well as inner political and economic adversities of Member-States, resulted into

the formation of a two-speed Europe with the developed countries accomplishing most of the objectives set, whereas the developing and the newcomers to EU countries have been lagged behind significantly. Hence, it is imperative on one hand to review the current situation and set a more realistic and achievable targets for all participants, and on the other hand, the participants to be more disciplined and punctual to their commitments in order to advance to the next level of policy making and regulation adoption. Otherwise, the most probable scenario is to be outweighed by the objectives themselves, to never reach a unified pan-european level of electronic services and to perpetuate the existing gap among Member-States.

#### 4. Greece

Greece has since the mid of 1990s proceeded towards catching up with the more advanced European countries in terms of using and facilitating the ICTs in all aspects of life economy, employment, commerce and, of course, public administration. The public sector in Greece founded in 1830s and throughout the years has kept somewhat its initial structure with strictly hierarchical relations, overflow of regulations and increased number of departments. The Greek public sector consists of the central and two levels of local government levels as well as a number of guangos/semi-public organisations and independent administrative authorities (Pettrakaki, 2008). The following table depicts the Greek public administration according to the new updated version of the “Register of Services and Organisations of Public Administration” as published by the Ministry of Interior, Decentralisation & E-Governance in March 2011 –after the implementation of “Kallikratis” law for the transformation of local administration:

STRUCTURE OF PUBLIC SECTOR	
Independent Public Services of Constitutional Leadership of State	Local Administration Organisations of A' and B' Degree
Public Offices of Juridical Operation of State	Municipalities & Prefectures Unions
Public Offices of Legislative Operation of State	Networks of Prefectures
Independent Administrative Offices	Municipalities & Prefectures Confederations
Ministries	Municipalities Unions
Decentralised Administrations	Municipal Legal Persons

Table 2: Greek public sector administration structure

As a Member-State of EU, Greece has the obligation to conform its policy, regulatory and legal frameworks with that of European Union. In that context, Greek

governments have been trying to develop the means with which the Greek public administration would move towards information society and e-government. The impetus for the use of ICTs in public administration started as part of 2<sup>nd</sup> and 3<sup>rd</sup> Community Support Framework periods. The efforts during the 2nd period (1994-1999) concentrated mainly to informational e-government web portals and to supply public administration with technological infrastructure in order for the employees to get familiar with technology and quit the traditional paperwork. During the 3rd period (2000-2006) some, but not much, transactional e-services were provided by the public administration (Markellos, 2007). The 4<sup>th</sup> programming period started with the launch of the National Strategic Reference Framework in 2007 designates the planning of EU Funds at national level for the 2007-2013 period.

All of the Frameworks comprised of several Operational Programs (OP), which allocated the European and national funds to the projects. However, many divergences to the implementation were observed between different public organisations and agencies mainly in the level of modernisation and provided services to the citizens, whereas even the public services that “lead” the developments have a lot of way for improvement in order to reach the European mean values. However after 17 years of the launch of the first OP “Kleisthenis”, Greece has advanced very slowly in implementing ICTs and Internet technologies to public administration. The reasons for this delay could be situated to the misallocation of the funds, to unsustainable projects, to erroneous management, lack of vision, unskilled personnel, detached and uncoordinated efforts. Nevertheless, some progress has been made as illustrated to the following table, which is not inclusive but it contains the milestone towards the realisation of e-government:

TIMELINE OF GREEK E-GOVERNMENT INITIATIVES	
Year	Initiative
1994	OP “Kleisthenis” for the modernisation of public administration for the period 1994-2000
1995	White Paper “Greek Strategy for the Information Society: A Tool for Employment, Development and Quality of Life”
March 1997	Adoption of “Strategic Plan for Administrative Reform”
February 1998	Launch of a national-wide call center for the application of certificates and administrative documents
February 1999	White Paper “Greece in the Information Society: Strategies and Actions”
2000	OP “Ariadni” for the improvement of public administration services delivered by regional and local administration
May 2000	OP “Politeia” for the public administration reform

End 2000	OP “Information Society” (OPIS) for the achievement of the objectives set in White Paper of 1999 and eEurope 2002
2001	Establishing “Information Society S.A.” an state-owned company tasked to monitor and support the implementation of OPIS
April 2001	Launch of government networks “Syzfexis” as a pilot project
Spring 2002	Launch of “Citizen Service Centres” as one-stop administrative shops
2002	Update version of White Paper “Greece in the Information Society: Strategies and Actions”
2004	Establishing the “Central Procedure Simplification Committee” tasked with the administrative reform
March 2005	OP “Politeia 2005-2007” a 3-year program for the re-establishment of public administration
November 2005	“Syzfexis” becomes fully operational
January 2006	“Digital Strategy 2006-2013” which conforms with Lisbon Strategy to help Greece to perform a “digital leap”
May 2007	Launch of the campaign “Digital Greece” for the familisation of Greek citizens with ICTs
September 2007	OP “Digital Convergence” for financing projects foreseen in Digital Strategy
December 2007	OP “Public Administration Reform” for financing interventions towards the upgrade of the institutional environment and the rationalisation of public administrative structures
February 2008	Establishing “Digital Aid S.A.” a non-profit company tasked to contribute to the achievement of specific individual objectives of OP “Digital Convergence”
December 2008	Institutionalisation of “Greek e-Government Interoperability Framework” as a cornerstone of “Digital Strategy” for the provision of e-government services
May 2009	Launch of “National Portal of Public Administration, Hermes”
March 2010	Re-designing of OP “Digital Convergence” principals, strategies and directions
January 2011	Public deliberation of the Bill on E-Government

Table 3: Timeline of Greek e-government initiatives

The two (2) operational programs that contributed the most to the implementation of ICTs to public sector and the training of employees in using them were the OP Information Society (OPIS) and OP Digital Strategy 2006-2013.

### ***Operational program “information society” (2000)***

At the end of 2000, the Greek State presented the OP Information Society (OPIS) 2000-2006 as the mechanism that would reduce the technological gap between Greece and the other Member-States. The aim was to accomplish the objectives of the previously published White Paper “Greece in the Information Society: Strategy and Actions”, and to conform and implement the objectives of EU initiatives eEurope 2002 & eEurope 2005. OPIS was an innovative horizontal program, with actions cutting across the government, which within the context of the 3<sup>rd</sup> Community Support Framework (CSF) allocated over 2.4 billion euros into the proposed actions.

The OPIS set two (2) general objectives (a) Citizens and quality of life for the improvement of the quality of life for the average citizen by actions in a range of critical sectors such as public administration, health, transport and the environment, and (b) Economic development and human resources for developing telecommunications infrastructure, supporting economic mechanisms and employment by making the most of new technologies, creating an education and training system adapted to the needs of the 21st century, and promoting Greek culture. Those objectives were based on the principals of innovation and entrepreneurship, democracy and personal freedoms, and equal opportunities and social cohesion (Operational Program “Information Society”). In order for the above mentioned objectives to be realised the OPIS was divided into four (4) Action Lines:

1. Education and Culture: aiming to introduce the digital media into schools and curricula and training the educational staff in using these media as well as using new technologies for promoting Greek culture.
2. Citizens and Quality of Life: introduction of ICTs and modernisation of public administration, health and welfare, environment and transportation in order to improve the daily quality of life of Greek citizens.
3. Digital Economy and Employment: promotion of e-business by exploiting the use of ICTs into production, skills upgrading, employment and tele-work –especially in what concerned the SMEs– aiming making the step towards the new economy.
4. Communications: support of the market liberisation, development of telecommunication infrastructure to remote areas for the provision of advanced service with low cost and accessible to everyone.

E-government was categorised under the Action Line 2 “Citizens and Quality of Life” putting it as top priority aiming to the improvement of the quality of public services through the development of online services and the use of ICTs so as to optimise and re-engineer the internal administrative procedures and the commu-

nication between public organisations at state, regional and local level, to support the training of the skills of public servants in using the new technologies, to establish geographical and environmental mapping and administrative information systems including the implementation of a National Land Registry, to promote and use of ICTs in the healthcare and welfare system both in providing improved services to the public and in re-organising its administration and finance, and finally to introduce telematics to land, sea and air transport.

In December 2008, a revised version of the OPIS was published with alterations in the Action Line 2 “Citizens and Quality of Life” and Action Line 4 “Communications” regarding the extension of those two action lines due to the catastrophic fires of the summer of 2007 in Greece. The alteration referred to two (2) axes (a) the development of ICTs for the prevention and treatment of similar situations, and (b) the use of ICTs for the mitigation of the negative implications of the conflagration to the four Prefectures. The OPIS is considered to be a successful action plan as most of the objectives and targets set have been implemented to one extend. Of course, there were observed cases of failures due to poor handling and resources misuses, but OPIS gave Greece the boost to realise a giant step towards closing the digital gap with the most advanced countries and climb to higher positions to the global classification on e-government assessment.

### ***Operational program “digital convergence” (2007)***

the OP Digital Convergence was published in September 2007 as a continuance of the OPIS to assist Greece to realise the “digital leap” in terms of productivity and quality of life in order to approach the other Member-States, as the results of the previous operational programs were not satisfactory. The low departure point for the new technologies constitutes the main cause for which a digital leap is required so as to recover the lost time and dynamically capitalize on the ICTs. In light of the above vision, the strategic objective for the OP Digital Convergence for the period 2007 – 2013 is described as ‘*Digital Convergence of the country with the EU, capitalizing on the new Information and Communication Technologies*’ (Operational Program Digital Convergence, 2007).

The OP Digital Coverage is part of the Digital Strategy 2006-2013 that substitutes the White Paper “Greece in the Information Society: Strategy and Actions”, also is incorporated in the National Strategic Reference Framework 2007-2013, and its interventions will be co-financed by the European Regional Development Fund and national resources. The strategic objectives are supported by Priority Axes that specify the actions and interventions at national level (Operational Program Digital Convergence, 2007):

1. Productivity enhancements by capitalising on ICT: reinforcement of new technologies penetration in the production combined with business innovations development through targeted interventions with particular emphasis on SMEs in order to enhance enterprises' productivity. The suggested interventions are expected to bring down public procurements cost, reinforce transparency, improve productivity and urge public sector suppliers to adopt new technologies in order to broaden their customer basis by providing electronic services to the public sector.
2. ICT and quality of life improvement: the primary aim is the equivalent and undiscriminated access of all citizens to new technologies, the availability of digital services to citizens as foreseen by e-Europe 2005 and i2010 in parallel with fighting digital divide, the utilisation of ICT to reinforce the participation of citizens to democratic procedures especially in cooperation with Non Governmental Organisations, and the promotion of Greek civilisation and culture worldwide.

The formal text of OP Digital Convergence is 248-pages long in which all the objectives and interventions intended to fulfill these objectives with specific time tables and resources allocation are described in a detailed analysis. However, the OP is still in progress so we cannot derive definitive conclusions, but the current government has shown its commitment in attaining the objectives of both the Lisbon Strategy and the Digital Strategy with several initiatives undertaken already such as the Electronic Medical Prescription and the Single Payments Authority. In this context, in March 2010 the OP Digital Convergence was set to public deliberation in order to redesign the initial strategies and directions. The new horizontal technological interventions adopted are the following (Special Secretariat of Digital Plan):

- Open data: increase of accessibility and sustainability of digital collections, added value services to citizens, and transparency
- Interoperability: substantial interoperability between the systems of administration, and creation of a single Service Registry
- Cloud computing and data centres: better and more economical allocation of public resources through the development of G-Cloud, and exploitation of private data centres
- Open standards: reinforcement and development of interoperability standards to every project of public administration
- Multi-channel distribution: improvement of service quality, service of citizens anytime to any place, and provision of specialised access to specific publication groups.

***Draft bill on electronic government (2011)***

in January 2011, the Ministry of Interiors, Decentralisation & Electronic Government presented the Draft Bill on E-Government, the first integrated legislative attempt of Greek State to institutionalise in a single text all components –administrative, social, political, policy, technical, ethical– that affect the seamless and equivalent access to government information and services with the use of ICTs and the Internet.

The scope (Article 1) of the Draft Bill is two-fold: (a) the recognition of the right of each individual and private entity to communicate and transact with the public organisations via the use of ICTs, and (b) the regulation of ICTs usage by public organisations within the scope and needs derived from their administrative operation and the support to exercise their powers and transactions. The application areas of the Draft Bill are set to four (4) main areas of interest (Article2): (a) the exercise of powers for issuing documents by public organisations with the use of ICTs, (b) the electronic communication between public organisations, (c) the electronic communication and provision of e-government services among public organisation and individuals and/or private entities, and (d) the accessibility of individuals or private entities to public electronic documents and their availability for further use.

The Draft Bill is constituted from 30 Articles, which make provisions for the most crucial administrative issues regarding e-government, creating a context that determines the responsibilities and rights of all sides involved as well as a defined framework on e-government within which both public administration and operators can legally perform their electronic transactions. One of the characteristics is that in case part of a process, act or transaction is completed with non electronic means, the law is applied to the part that is processed electronically (Article 2 §2). Also, the Law is governed by the principals of legitimacy, good governance, transparency and authenticity, whereas sees to the security of systems and data, the availability of licenses and government information, and the user-friendly applications with care for the access of special populational groups such as the disabled or the elderly. (Article 4 §1-7).

The Draft Bill is divided in Sections each one covering a specific topic on a number of representative Articles. Articles 5 and 6 refer to the information obligations of public administration regarding the publishing, availability, accessibility, accuracy and updating of government information. In continuance, the Articles 7 to 10 describe the personal data privacy in accordance with the Law 2472/1997, the accessibility right to public information in accordance with the Article 5 of Law 2690/1999, and the right to use ICTs and electronic communication with public administration. Especially to personal data privacy, it is explic-



itly mentioned that “further usage of personal data than this of statistical reasons or for the improvement of the provided services is permitted either by doing the data anonymous or with the writing consent of the interested part” (Article 8 §1).

Further, Articles 11 to 18 define the context in which electronic administrative acts will be executed and the electronic public documents will be considered as legal and bearing validity and probative value, with specific reference to the compulsory use of digital signatures and the presence of timestamp to every document generated electronically by the public administration (Article 12). Also, Article 18 explicitly defines that all public organisations must employ ICTs under the scope of Greek e-Government Interoperability Framework, which is subject to revision by the Minister of Interiors, Decentralisation & E-Government when deemed necessary.

Articles 19 to 25 describe the electronic communication, distribution of documents and financial transactions among public administration and individuals and/or private entities, which are considered valid only when abide the conditions of authenticity and identification as well as security policy of each public organisation (Article 19 §2). Finally, Articles 26 to 30 refer to obligation of authenticity and identification in order to conduct an electronic communication of any kind with public administration, the exceptions to that rule, and the process of acquiring the required identifiers. As a general rule, authenticity and identification of the enacting part is required for each act that originates legitimate effect (Article 27). The exception of this rule is when the information communicated is generally accessible to everyone such as guidelines, studies, reports, statistical data, newsletters etc. (Article 26 §1).

The E-Government Bill is the first legislative text of Greek State dedicated entirely to e-government. However, many points have not been clarified and are subjected to further regulatory and legislative context. Also, the E-Government Bill is applied in accordance with a number of other laws of Greek State as Law 2472/1997 & Law 3471/2006 on Data Protection/Privacy Legislation, Presidential Degree 131/2003 on E-Commerce, Presidential Degree 150/2001 on Electronic Signatures, Presidential Degrees 59/2007, 60/2007 & 118/2007 on Electronic Procurement, Law 3448/2006 on Re-use of Public Sector Information.

By the time of the writing, the Draft Bill is still under elaboration in which the task force reviews and evaluates the results of the public deliberation. Nevertheless, it is expected that it will be improvements but the core will remain to the initial path.

## 5. Conclusions

As demonstrated, the route that US, EU and Greece followed towards the development and implementation of e-government is quite different and diverse. However, but targets and results expected were the same with predominant the reformation of public administration with the use of ICT aiming to provide on-line, seamless, equal, continuous, horizontal, agency independent and qualitative access to services.

US has been a leader in introducing ICT and Internet technologies to public administration and has been accompanied this effort by regulatory and legislative framework since the early 1990s by adopting a number of relative laws with the most important the E-Government Act of 2002 and the current Open Government. Nevertheless, this effort was not without failures on the way, but US seem to present the most consistent and innovative approach on e-government policy.

On the other hand, EU has delayed to undertake initiatives regarding e-government compared to US. A legal characteristic of EU is that depending on the type of legislation –regulation, directive or decision– lays upon each Member-State's discretion how it will be adapted to national law. Consequently, a piece of legislation is possible to be introduced diversely between Member-States –especially concerning the directives which are not obligatory and are transferred to national legislation as deemed appropriate. Under this scope, EU adopted successive policy initiatives to guide its Member-States towards an inclusive, integrated Information Society and to level off the differences and disparities among Member-States. *eEurope* and *i2010* initiatives aimed to exploit in full the potentials that the Information Society had to offer in conjunction with a transformation of the economy, the society and the culture of Europe.

Finally, Greece has been lagged behind both in harmonising its national law to EU recommendations and exploiting successfully the funds provided by EU to modernise and re-engineer public administration. However even with the delays and the mismanagement, we can definitely say that Greece has come a long way from the starting point at the middle of 1990s with the most recent example the recent published Draft Bill on E-Government. The vision and the wish focus on the efforts to continue with more intensive rate in order to catch up with the rest more advanced countries worldwide.

The common element to US, EU and Greece –and basically to all developed countries– is that have recently begun to realise the enormous opportunities that e-government has to offer, but still they remain to an infantile level both from legislative and regulatory aspect as well as the penetration of applications. The interest focuses on how governments can materialise the constant changing and

revolutionary nature of e-government to accomplish their mission, namely to serve their citizens with an efficient and effective way.

## References

Criado, I. (2009), Europeanization of e-government policy: institutional mechanisms and implications for public sector innovation, *Information Polity*, 14, 299-314.

European Commission (1999), eEurope – An information society for all, online at [http://europa.eu/legislation\\_summaries/information\\_society/l24221\\_en.htm](http://europa.eu/legislation_summaries/information_society/l24221_en.htm) / accessed 15.04.2011.

European Commission (2000), eEurope 2002 – An information society for all, online at [http://ec.europa.eu/information\\_society/eeurope/2002/documents/archiv\\_eEurope2002/actionplan\\_en.pdf](http://ec.europa.eu/information_society/eeurope/2002/documents/archiv_eEurope2002/actionplan_en.pdf) / accessed 15.04.2011.

European Commission (2002), eEurope 2005 – An information society for all, online at [http://ec.europa.eu/information\\_society/eeurope/2002/news\\_library/documents/eeurope2005/eeurope2005\\_en.pdf](http://ec.europa.eu/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf) / accessed 16.04.2011.

European Commission (2005), i2010 – A European information society for growth and employment, online at [http://www.epractice.eu/files/media/media\\_212.pdf](http://www.epractice.eu/files/media/media_212.pdf)/accessed 16.04.2011.

European Commission (2006), i2010 eGovernment action plan: accelerating eGovernment in Europe for the benefit of all, online at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0173:FIN:EN:PDF>/accessed 16.04.2011.

European Commission (2010), eGovernment in Greece, online at [http://www.observatory.gr/files/meletes/eGovernment\\_in\\_GR\\_April\\_2010\\_en.pdf](http://www.observatory.gr/files/meletes/eGovernment_in_GR_April_2010_en.pdf)/accessed 18.04.2011.

Fang, Z. (2002), E-Government in digital era: concept, practice and development, *International Journal of The Computer, The Internet and Management*, 10(2), 1-22.

Fletcher, P. D. (2002), The Government Paperwork Elimination Act, *International Journal of Public Administration*, 25(5), 723-736.

Hagen, M. (2004). Electronic government in the United States, in *National electronic government*, edited by Eifert, M. and Puschel, Jan Ole, Routledge, 211-241.

Liinkanen, E. (2003), eGovernment: an EU perspective, *Journal of Political Marketing*, 2(3-4), 65-88.

Markellos, K et al (2007), Current state of greek e-government initiatives, *Journal of Business Systems, Governance and Ethics*, 2(3), 67-88.

Milward, B. H., and Snyder, L. O. (1996), Electronic government, *Journal of Public Administration Research and Theory*, 6(2), 261-275.

National Performance Review (1993a) From red tape to results: creating a government that works better and cost less, online at <http://govinfo.library.unt.edu/npr/whoweare/historypart1.html> / accessed 29.03.2011.

National Performance Review (1993b), Reengineering through information technology (2001), online at <http://govinfo.library.unt.edu/npr/library/reports/it.html> / accessed 29.03.2011.

Operational Program Information Society (2001), REGIO/2001/00227-00-00, online at [http://www.epractice.eu/files/media/media\\_406.pdf](http://www.epractice.eu/files/media/media_406.pdf) / accessed 18.04.2011.

Operational Program Digital Convergence (2007), 2007GR161PO002, online at [http://www.espa.gr/elibrary/Episimo\\_Keimeno\\_EP\\_Psifiaki\\_Syglisi.pdf](http://www.espa.gr/elibrary/Episimo_Keimeno_EP_Psifiaki_Syglisi.pdf) / accessed 18.04.2011.

Petrakaki, D. (2008). E-government and changes in the public sector, in *Information Technology in the service economy: challenges and possibilities for the 21st Century IFIP International Federation for Information Processing*, 213-227.

Radin, B. A. (1998), The Government Performance and Results Act (GPRA): Hydra-headed monster of flexible management tool?, *Public Administration Review*, 58(4), 307-317.

Radin, B. A. (2000), The Government Performance and Results Act and the transition of federal management reform: square pegs in round holes?, *Journal of Public Administration Research and Theory*, 10(1), 111-135.

Seifert, J. W., and Petersen, R. E. (2002), The promise of all things E?: expectations and challenges of emergent electronic government, *Perspectives on Global Development and Technology*, 1(2), 193-212.

Seifert, J. W. (2008), Reauthorization of the E-Government Act: a brief overview, CRS report for Congress RL34492, online at <http://www.fas.org/sgp/crs/secrecy/RL34492.pdf> / accessed 14.04.2011.

Special Secretariat of Digital Plan, Operational Program Digital Convergence, online at <http://www.digitalplan.gov.gr/portal/resource/section/Epiheirhsiako-Programma> / accessed 18.04.2011.

U.S. Chief Information Officers Council (1998), Government Paperwork Elimination Act, 44 USC 3504, online at [http://www.cio.gov/Documents/paperwork\\_elimination\\_act.html](http://www.cio.gov/Documents/paperwork_elimination_act.html) / accessed 14.04.2011.

U.S. Congress (2002), E-Government Act., HR2458, PL 107-347, online at <http://csrc.nist.gov/drivers/documents/HR2458-final.pdf> / accessed 14.04.2011.

U.S. Congress (2007), E-Government Reauthorization Act of 2007, S.2321, online at <http://www.gpo.gov/fdsys/pkg/BILLS-110s2321is/pdf/BILLS-110s2321is.pdf> / accessed 14.04.2011.

U.S. Office of Management and Budget (1993), Government Performance Results Act of 1993, online at <http://www.whitehouse.gov/omb/mgmt-gpra/gplaw2m> / accessed 01.04.2011.

U.S. Office of Management and Budget (2009), Open Government Directive, M-10-06, online at <http://www.whitehouse.gov/open/documents/open-government-directive> / accessed 15.04.2011.

U.S. White House (2009), Transparency and open government, Memorandum for the Heads of Executive Departments and Agencies, online at [http://www.whitehouse.gov/the\\_press\\_office/TransparencyandOpenGovernment](http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment) / accessed 14.04.2011.

Zobel, Rosalie (2005), E-government: European Commission policies and activities, in *Online citizenship*, Springer, 7-22.





