# An Information Law for the 21st Century

**An Information Law for the 21st Century**
ISBN 978-960-272-791-1

**ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ**
Μαυρομιχάλη 23, 106 80 Αθήνα
Τηλ.: 210 3678 800 • Fax: 210 3678 819
http://www.nb.org • e-mail: info@nb.org

*Αθήνα:* Μαυρομιχάλη 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



*Art Director:* Θεόδωρος Μαστρογιάννης
*Υπεύθυνος Παραγωγής:* Ανδρέας Μενούνος
*Φωτοστοιχειοθεσία:* Αριστέα Διακουμοπούλου
*Παραγωγή:* NB Production AM100111M23

**NOMIKI BIBLIOTHIKI 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

Third International Seminar
on Information Law 2010

Edited by Maria Bottis

# An Information Law for the 21st Century

Ionian University, Corfu, Greece
Department of Archive and Library Science

International Society for Ethics and Technology
Institute for Legal Informatics

NOMIKI BIBLIOTHIKI

On behalf of INSEIT, I am delighted to congratulate Ass. Professor Maria Bottis, who has once again put together another highly successful conference in the ISIL series. INSEIT, the International Society for Ethics and Technology, has been a proud sponsor of ISIL 2009 and ISIL 2010, and is pleased to serve as a sponsor for the ICIL 2011 Conference, which will be held in Thessaloniki next May. I personally have enjoyed working closely with Ass. Professor Bottis who, I believe, has also done an outstanding job of forging a strong professional connection between the ISIL conference series and INSEIT, and between that conference series and the CEPE (Computer Ethics: Philosophical Enquiry) series, which is also sponsored by INSEIT. I look forward to working with her to continue to strengthen the relationship between these professional organizations and conference series.

Herman T. Tavani
President, INSEIT

# Contents

## Young Scholars Forum

## Organizing Committee

Anastasiou Nikos, Konsta Rania, Mavrona Maria, Siameti Gianna, Tzali Katerina

## Program Committee

Alexandropoulou-Aigiptiadou Jenny, Associate Professor, University of Macedonia

Bitsani Evgenia, Associate Professor, Technological Educational Institute of Kalamata

Bokos George, Professor, Ionian University

Bottis Maria, Assistant Professor, Ionian University

Capurro Rafael, Professor, Stuttgart University

Chryssikopoulos Vassileios, Professor, Ionian University

Floridi Luciano, Professor, University of Oxford-University of Hertfordshire

Gritzalis Dimitris, Professor, Athens University of Economics and Business

Grodzinsky Frances, Professor, Sacred Heart University

Himma Kenneth Einar, Professor, Seattle Pacific University

Kallinikou Dionysia, Professor, University of Athens

Karachalios Konstantinos, Scenarios Analyst, European Patent Office

Karakostas Ioannis, Professor, University of Athens

Kavoura G. Androniki, Assistant Professor, Technological Educational Institute of Athens

Kostagiolas Petros, Lecturer, Ionian University

Kotsiris Lambros, Professor emeritus, University of Thessaloniki

Mitrou Lilian, Assistant Professor, University of Aegean

Papadakis John, Lecturer, Ionian University

Papavlassopoulos Sozon, Adjunct Lecturer, Ionian University

Pateli Ada, Lecturer, Ionian University

Poulos Marios, Assistant Professor, Ionian University

Spinello Richard, Professor, Boston College

Tavani Herman, Professor, Rivier College

Vlamos Panayotis, Assistant Professor, Ionian University

## Postgraduate Students (Class of 2010-2011)

Barka Polixeni, Christodoulou Elena, Ganatsiou Paraskevi, Kanlis George, Karagianni Paraskevi, Kiritsi Margarita, Kontostanou Stefania Maria, Korakianiti Spiridoula Sofia, Kritikou Irini Maria, Lavranos Charilaos Stylianos, Magoula Irini Sofia, Marouli Tania, Meti Aggeliki, Nikopoulou Maria Eleni, Pairamidou Spiridoula Maria, Palamioti Stella, Palli Aggeliki, Papadaki Evaggelia, Papadopoulou Katerina, Papapostolou Maria, Spyrou Maria, Stavrakis George, Vais Panayotis, Vlahou Paraskevi, Zarogianni Stavroula. Thank you all. As you know, ISIL 2010 was devoted to you.

## Notes on the 3rd International Seminar on Information Law 2011

This volume contains the proceedings of the 3rd International Seminar on Information Law 2011 which took place in Corfu, June 26-28, 2010. The third Seminar was "larger" in every sense from the 1st and the 2nd International Seminars; more than thirty five scholars presented their research on many diverse aspects of information law and ethics and more of our Department's students attended, as we have had many people from previous postgraduate classes who returned in Corfu for the Seminar. This time, also, the Seminar was not only sponsored by INSEIT (the International Society for Ethics and Technology) but additionally by the German Institute for Legal Informatics (IRI). I express here my gratitude for the honorable support from both these organizations. Thank you Pr. Tavani, thank you Pr. Forgó.

The Vice-Rector of the University of Athens, Professor Ioannis Karakostas officially opened the Seminar. He also delivered a lecture at Corfu Reading Society as a pre-seminar event titled "*Personality and Environment*". Thank you so much Pr. Karakostas for your kind support and participation-a very great honor.

Our keynote speakers, President Commissioner Oscar Guerra Mauricio Ford, Head of the Mexican Institute for Access to Public Information for the Federal District, Professor Lambros Kotsiris, Member of the Greek Academy and honorable Chair of ISIL 2010 and Dr. Konstantinos Karachalios, Scenarios Analyst for the European Patent Office delivered excellent presentations of their topics. In this volume, we print their work for the Seminar. I thank from my heart President Commissioner Ford as he came, with his wonderful wife Alicia, from so far away to our island to meet our students and speak to us about Mexico and the Institute's work. I also owe special gratitude to our interpreter, Theodore Buchellos; without him, and his professional team, the presentation of Commissioner Ford would not have been possible. I need to stress that Pr. Kotsiris and Dr. Karachalios returned to Corfu, as they had honored us also in 2009, for the Second International Seminar on In-

formation Law. Thank you so much for such a vote of confidence. Ass. Professor Lilian Mitrou also presented the current evolutions of the European privacy law, as a respondent to President Commissioner's speech; thank you Lilian. Ass. Professor Angelos Syrigos introduced Ass. Pr. Mitrou - thank you Angelos.

Many speakers had also presented their work or attended the Second Seminar. We are all grateful for their steady support. In this third Seminar we started a call for papers and the Young Scholars' Forum for the first time, in which our young scholars (PhD candidates, Master students) had the chance to present their work and exchange ideas with the foreign and Greek scholars who participated in ISIL 2011. In ISIL 2011, we hosted scholars from Brazil, Italy, Russia, Servia, United Kingdom, USA and other countries.

I thank all member of the organizing committee (Anastasiou Nikos, Konsta Rania, Mavrona Maria, Siameti Gianna, Tzali Katerina) for their care. From the postgraduate calls, many students offered excellent voluntary support, Pairamidou Spiridoula-Maria, Spyrou Maria, Vlahou Paraskevi, Zarogianni Stavroula, Magoula Sofia-and others. Thank you all, very much. Alexandros Panaretos was in charge of the technical support of ISIL 2010-without him and his team, we wouldn't be able to run it. Thank you Alexandros. Dionysis Kourtesis designed our brilliant poster and banners-thank you Dionysis.

Dr. Andreas Giannakopoulos worked very hard and with impressive professionalism and artistic imagination on the Seminar's site. The site was, of course, our connection to the world and as we all know, a site always plays a major role in any event's success. I cannot thank Andreas enough, ever, for all these long (and late) hours of care of the ISIL site. You can find there important information about the Seminar and a very large collection of photos. Marina Kontzali, a graduate of our Department and a professional photographer was responsible for all photographs in the site. Thank you Marina, for selecting to capture all those artistic, genuine and spontaneous aspects of the Seminar. Nomiki Vivliothiki, our publisher, sponsored the event, as every year; thank you very much for your constant support.

I thank Rector Dimitris Tsougkarakis and Vice-Dean Vassilis Chryssikopoulos for their support.

The third ISIL 2010 would not have taken place without the encouragement of Professor George Bokos, who had supported it from the very beginning. Thank you Professor-the Seminar is, very truly, "due" to you, as you, as Chairman of the Postgraduate Class, allowed it to be born in 2008 (and offered a very generous financial stipend for it). I cannot express my gratitude properly enough.

I also thank very much the Chairman of DALS, Professor Theodore Pappas and the Chairman of the 2010-2011 Postgraduate Class, Professor Spiros Asonitis, for their help. I thank you both for everything.

I thank our faculty members for their support and for attending the Seminar.

I also thank all students of the undergraduate class on Information Law, who offered valuable voluntary work for the Seminar.

The next event is the International Conference on Information Law 2011, in Thessaloniki, as a collaborative event with the University of Macedonia and the Aristotelian University in Thessaloniki an especially, the Law School. We invite all scholars and students interested in the field of information law and ethics to participate, in May 2011 in Thessaloniki, Greece.

Maria Bottis
Assistant Professor
DALS, Ionian University
Corfu, November 2010

# Protecting patients' rights in clinical trial scenarios: The "bee metaphor" and the simbiotical relationship

**Marcelo Corrales**

## Introduction - The 'bee metaphor'

Genetic data is regarded as having the potential of revealing in the future, scientific, medical and personal information of each individual. It can also reveal some singular characteristics in particular compared to health data. This information can be extended to the family of the data subject. It is therefore regarded to be unique as it is likely to reveal information of many people by identifying only one of them (Article 29 Data Protection Working Party, 2004 but see also Bottis, 2000). For instance, the queen bee enjoys a unique status in the hive although having exactly the same genome of the rest of the bees. There is only one queen bee in the hive, between 500 to 1.000 drones and about 30.000 to 60.000 worker bees. The uniqueness of the queen bee can be easily determined at first sight as she is in principle the largest bee of the colony. She is also able to control other bees by secreting a particular substance, a pheromone that manipulates the activities and behaviours in the hive. Genetically, and due to her large abdomen which extends to the tips of her wings, she is the only sexually developed female in the hive being able to lay up to 2000 eggs per day. The queen bee is nurtured on a special diet of royal jelly which is collected by the worker bees also known as "forgarers" (Kirchberger, 2005).

In a bee world scenario, the forgarers fly around the hive collecting the pollen from the flowers and through a fascinating dance called the "waggle dance" they communicate to the rest of the bees where the flowers are located. The more they waggle the more flowers are supposed to be in the place they are facing, using the sun as an indicator for orientation (Herms, 1990).

This article has been inspired and motivated by the EU research project Advancing Clinico Genomic Trials on Cancer (ACGT www.eu-acgt.org), the main purpose of which is to develope a grid based technology in support of a trans-European post-genomic clinical trial research on cancer. By analogy, the "bee metaphor" applies directly to a clinical trial scenario where the forgarers or worker bees represent the scientists who collects genetic data from the flowers which represent groups of patients. That is, within a clinical trial scenario a computing grid infrastructure is used to tell the scientist where is the best and easiest way to access the genetic data

they are searching for in the same way a worker bee tells the other forgarers where the flowers are by performing the so called "waggle dance".

Finally, in the same way a hive of bees is extremely protected by the other co-workers bees, because of the "uniqueness" and "sensitivity" of genetic data in a clinical trial scenario, this must be protected and secured according to data protection legislation.

## Protecting patient's privacy – The ACGT scenario

Genetic research projects within clinical trials scenarios need to safeguard patients' rights. Hence, a data protection framework needs to be developed where the handling of patients' genetic data is in compliance with the data protection legislation.

In ACGT the biological data collected from the patients is stored in different hospitals. Then this data is collected and then anonymized with a special encryption tool called CAT. Once data has been anonymized, it is ready for its usage among researchers. In order to guarantee compliance with the data protection legislation it is essential to put, in a first step, the project consortium in the position able to audit such compliance. For this reason it is important to establish a data protection authority in charge of engaging with both the patients on the one hand, and the end users i.e. researchers on the other. In ACGT the Center for Data Protection (CDP www.privacypeople.org) is able to sign contracts between the main stakeholders which is independent to the project consortium and empowered to inflict a penalty for infringement. Under this framework, patients who would like to contribute data, are able to sign a data transfer agreement in order to release their data to the researchers and conversely, researchers must sign a legally binding contract on data protection and data security in order to get access to data. Both agreements give the CDP the power to inflict pecuniary sanctions and therefore enforce compliance with the data protection framework. In addition, the CDP acts as a data controller acting as a central contact point for those patients and researchers (Claerhout et al, 2008).

All biological data collected and processed by ACGT is due to the cooperation of patients who consent to transfer their data on behalf of scientific research hoping that ACGT scientific efforts will foster and promote future scientific research for their diseases such as the nephroblastoma (Wilm's tumour) and eventually find a possible cure for this disease. In our "bee metaphor" the pollen is collected from the flowers and then is taken to the hive. The more pollen that is collected, the more nectar and honey will be produced in the hive. In the same way, the more biological data is collected within a clinical trial scenario, the more chances scientists will have to find a cure for diseases like cancer.

For this reason, clinical trial research projects such as ACGT owes its existence to the input of patients. Without their genetic samples and its associated information such collection of biological data would simply not exist (Gesche, 2006). It is evident that both, researchers and patients have a general common interest of finding the cure for a particular sort of disease (Lenk, 2009). Nonetheless, this relevant interest can take different positions. Namely, in respect to ACGT on the one hand, there is an essential interest for the patients to develop a successful treatment for their disease. On the other hand, there is a special attention on the side of the researchers to use such data in order to carry on with their research.

In the following section, I describe the two cases which constitute a land mark concerning the relationship between patients and scientists. These cases expounded below clearly show the conflicts of interest between the parties involved and suggest the acknowledgement of patients' rights.

## The Greenberg case

The Greenberg Case (*Greenberg et al. v. Miami Children's Hospital Research Institute Inc. et al.,* 2003) is about a hereditary disease called Canavan which manifests in early childhood. The disease is usually rare, occurring in 1 of 6400 children (Lenk, 2009). This case consists of a joint legal suit of parents and non-profit organizations who found medical help in a group of researchers from the Miami Children's Hospital.

This group of parents (the Greenberg group) of children suffering of Canavan disease, working with specialists from the Miami Children's Hospital aided to collect samples of blood and tissues and create a database together with the hospital. The database contained clinical and medical data about the families and supplied this collection of data to Dr. Matalon. With all this information Dr. Matalon and his research team managed to isolate the gene responsible for Canavan disease, thus filing a patent application for the genetic sequence for the Canavan gene who successfully established a restrictive patent licensing program. Therefore, the Greenberg group, which had assumed that the benefits of Dr. Matalon's research would be in the public domain in order to foster future research, had also contended a claim for conversion on the grounds of property rights in the tissues and associated biological information provided to Dr. Matalon (Evans, 2006).

The plaintiffs (Greenberg group) filed a complaint based in a number of legal grounds claiming property rights not just to the corporeal tissues but "the genetic information therein" and information contained in Canavan Register (Mason et al, 2002). At the end, the Canavan Foundation lost the legal proceedings (Lenk, 2009) but reached a confidential settlement which provides for a continued "royalty-based genetic testing" by some licensed laboratories and "royalty-free"

research by doctors, scientist and institutions searching for a possible cure (Canavan Joint Press, 2003).

It follows from the foregoing situation that the crucial point constitutes the question of who has the legal or moral rights for the intangible or intellectual property rights rather than who is the legal owner of the tangible property such as the tissues samples (Lenk, 2009).

## The Moore case

In the same vein, another interesting case law worthy to mention is the Moore case. In this case, the plaintiff John Moore participated in a treatment for hairy-cell leukemia at the Medical Center of the University of California (*John Moore v. The regents of the university of california et al*. Supreme Court of California, 1990). After repeated medical studies over Moore's bodily substances, his treating physician Dr. Golde suggested to extract his spleen for further research purposes rather than for medical tests without Moore's express consent. After the surgery John Moore was asked to come to UCLA Medical Center for further tests where a great deal of bodily substances coupled with its associate biological information were removed for further research (Rainbow, 2002).

Dr. Golde found a number of potentially therapeutic purposes in Moore's cells which were grown in culture. Moore's cells were commercially important since they produced a particular sort of protein which could be further industrialized at a lower cost. As a matter of fact, Golde and the University of California obtained a patent on the cell line and profited from an arrangement with a biotechnology company (Science News Article Moore 1988). Moore filed a complaint including different legal actions such as conversion, lack of informed consent, unjust enrichment, breach of fiduciary duty, etc. (*Moore v. Regents of University of California,* 1990).

Finally, the Decision was against John Moore who did not get any profit out of his bodily substance and associated information. Accordingly, from the aforementioned cases illustrated above, within the context of clinical trials a crucial question must be answered: What is the significant contribution for the obtaining of scientific knowledge: is it the biological data obtained from patients or the investment of substantial research work and previous medical knowledge from the researchers? Therefore, a proportional distribution must be sought, and we can arrive to the conclusion that patients taking part in clinical trials must receive something in return to their contributions (Lenk, 2009).

## Balancing interest rights between patients and researcher

This section will analyze the proper distribution of rights between the interest of patients giving their data within a clinical trial scenario and the researchers producing results out of these data taking as an example the ACGT project. Below I briefly describe several options highlighting the pros and cons. At the end, the best equilibrium will be proposed.

## Individual feedback to patients

From the patient's side a financial compensation must never be sought in advance. Instead, the first step is to grant patients the right to access the scientific results so they can control the progress of the ongoing clinical trials which is a product of a joint cooperation between the patients and the researchers (Lenk, 2009).

In this respect, ACGT is consistent with regards to providing access to patient's clinical records who are be considered as a clinician with limited access to their own various summaries of the findings coupled with their own clinical data.

## Access to innovative therapeutic or diagnostic methods

The right to know about any new therapeutic or diagnostic methods is an ethical principle which is backed up by the Declaration of Helsinki (Lenk, 2009). Paragraph 30 states as follows, "At the conclusion of the study, every patient entered into it should be assured of access to the best proven prophylactic, diagnostic and therapeutic methods identified by the study". The Declaration of Helsinki is not a legally binding instrument; however, since it was drafted by the World Medical Association, it is a respected ethical document.

## Improvement of health care in a specific category of patients

In cases of uncommon diseases such as Wilm's tumour (nephroblastoma) cancer it may be an alternative to share the results in an improved group health care benefit. This is usually the case with a particular group of patients from a determined region (Lenk, 2009). In ACGT, the improvement of the health care sector in a particular region where clinical trials are in process can be an interesting alternative in order to find a balance between the interest of the researchers and patients. Building e.g. a therapy method or infrastructure within the hospitals and group of patients participating in ACGT cannot only provide a proper balance of interest between patients and researchers, but can also suggest future funding revenues at national level taking into account that benefits will be shared within the community where the patients are located.

## The "Contractual Model"

This model has been presented by Gerard Porter whereby – due to the reposition of the traditional research model to the new commercial research paradigm – informed consent has been adjusted to a new setting where the dual worlds of intellectual property and bioethics converge (Porter, 2004). This model puts forward a balance between patients and researchers through the bargain of terms and conditions. Normally, informed consent forms are employed as a procedural and bureaucratic matter to waive participant's right to claim any potential intellectual property compensation whilst they should rather be used as an instrument to safeguard the balance between the interested parties in play (Porter, 2004).

According to Porter, informed consent forms are like a "wolf in sheep's clothing" since the wordings described therein are usually camouflaged by the real commercial intentions. Informed consent forms resemble the typical standard contracts between big companies and their clients where no room for negotiation is provided having only the chance to participate or not within the terms of the contract. For this reason, he proposes a wider room for negotiation where in particular, the researchers must inform the potential commercial intellectual property values of their biological material and associated information (Porter, 2004).

## Distribution of financial profits

It has been previously said that a direct financial compensation must never be sought in advance (see above section 3.1.). In spite of this, an indirect compensation for patients can be seen in the distribution of financial profits. The recommendations of the Human Genome Organization's Ethics Committee are a good example, as it has plausibly suggested that "profit-making entities dedicate a percentage (e.g. 1-3%) of their annual net profit to healthcare infrastructure and/or to humanitarian efforts" (Laurie, 2003).

By analogy, clinical trial research projects such as the ACGT project may consider to find a similar solution with regard to the interplay between patients and hospitals as a means of distributing potential financial profits i.e. researchers may devote a percentage of their profits to health care infrastructure for the patients.

### *2.1. The "Taxation Model"*

This model has been recently proposed by Jasper Bovenberg who presents an interesting system based on taxes. He proposes to set a tax rate specifically tailored for tissues and cell products. This model rests in the fact that human tissues constitute a natural resource and has been inspired by the United Nations Convention on the Law of the Sea regarding the tax imposition of any removal from the mineral sourc-

es of the deep seabed. In this convention, a trust fund called the "Deep Seabed Revenue Sharing Trust Fund" was established. The main idea is to consider by analogy that genetic material and associated biological information can be contemplated as a "global public good", therefore the tax must be "global" or at least run by a national authority as it is the case with the Netherlands with regard to mine minerals, oil or natural gas taken from Dutch territory (Bovenberg, 2006).

This is an interesting model to consider, however, it might be difficult to implement within small projects. The major drawback is the international or at least national necessary lobby to obtain a taxation rate and an authority empowered to collect and control taxes.

## The "Charitable Trust Model"

This model takes for granted property rights in patient's biological material and associated data. Although it has not been effectively implemented yet, it provides an interesting benefit-sharing approach by designating a 'charitable trust' which will have 'legal fiduciary duties' to hold or use the property on behalf and benefit of the public. By means of this model, donors would co-participate in the governance of the trust and be entitled to some shares ruled by the terms and conditions of the trust agreement (Bovenberg, 2006, Tavani & Bottis 2010).

## Conclusion

The fascinating social behavior of honey bees suggests that bees are not the only one benefiting from the collection of pollen but many plants depend on the pollination for their very survival. Bees and other insects have built up a symbiotic relationship with nature. Respectively, the "bee metaphor" resembles the relationship between patients and researchers where not only researchers receive the scientific and economical benefits from the biological data taken from patients but there is a rather mutual relationship where the group of patients including their communities should receive some benefits too.

This relationship should be built up through a bilateral manifestation between patients and researchers in terms of a contractual agreement where the principle of 'freedom of contract' fulfills the purpose of safeguarding the autonomies of the interested parties.

The Greenberg and the Moore court rulings depicted above clearly manifest how patients and participants of clinical trial scenarios have seen their rights considerably undermined therefore several models to balance these rights have been examined. The list given above in Section 3 is by no means exhaustive but illustrative. Technically speaking some of these models do not apply directly to

some clinical trial scenarios however a number of these models can provide useful guidelines for our discussion.

In this sense, we suggest a model based on an equal balance between the interested parties, and in particular, a more active participation of patients. This is due not only to ethical and legal reasoning but it actually can encourage the participation of patients which represent the sources of information for achieving the scientific outcomes of the ACGT project.

For practical reasons, as a central authority is needed for data protection and data security issues anyway, this institution may also be used for other central tasks. For instance, taking care of the patient's possible intellectual property rights regarding their biological data, being able to establish a refund model in order to share the benefits within the consortium and the group of patients which can be extended to the community where those clinical trials are taking place.

For this reason, the CDP could also act as a "Trusted Party" and could define property rights on the biological material and the data coming out of this material as a "common". In order to find a balance between the interests of patients, doctors and researchers, the CDP as the "Trust" could hold a percentage of the net profits and re-distribute the revenues to the community of patients.

## Acknowledgement

The results presented in this paper are partially funded by the EU 6th Framework Program in the context of the ACGT project (FP6-IST-026996). The author wants to thank all who contributed to this paper, especially the members of the project consortium and in particular Prof. Nikolaus Forgó who supervised the entire work package concerning legal and ethical issues and to my colleagues Dr. Tina Krügel and Dipl. Jur. Eva Egermann, LL.M. Last but not least, I would like to thank Mike Wilson for the corrections made to this article including his valuable feedback on the content. However, the usual disclaimer applies. The content of this article does not necessarily reflect the views of the Institute for Legal Informatics. The author is solely responsible for its content.

## References

Article 29 Data Protection Working Party, Working Document on Genetic Data adopted on March 17 2004, 1-14.

Bovenberg J. (2006) Property Rights in Blood, Genes and Data: Naturally Yours?, 197.

Claerhout B., Forgó N., Kruegel T., Arning M., de Moor G. (2008) A Data Protection Framework for Transeuropean genetic research projects in Collaborative Patient Centred eHealth, 67-72.

Evans P., Patent Rights in Biological Material: Implications of Principle of Unjust Enrichment Remain Uncertain, (2006) GEN Genetic Engineering and Biotechnology News, Vol. 26, No. 17, 1.

Gesche A., (2006) Genetic Testing and Human Genetic Databases, in Betta, Michela, Eds. The Moral, Social, and Commercial Imperatives of Genetic Testing and Screening: the Australian case, chapter 4, pages (Abstract), Springer (2006) at http://eprints.qut.edu.au/archive/00006360, accessed 29.05.2010

Herms D., (1990) The Honey Bee Waggle Dance: An Active Participation, Role Playing game (1990), Entomology Notes No. 22 at http://insects.ummz.lsa.umich.edu/MES/notes/entnote22.html, accessed 29.05.2010.

Kirchberger C., (2005) The Queen Bee metaphor – the existence of a law as a unique instance", at www.lisan.org/li/docs/archive/TheQueenBee_metaphor.pdf, accessed 29.05.2010

Laurie G., (2003) Privacy and Property? Multi-Level Strategies for Protecting Personal Interests in Genetic Material, p. 85 in Genomics, Health and Society: Emerging Issues for Public Policy edited by Bartha Maria Knoppers and Charles Scrivers published by the Policy Research Initiative, Canada.

Lenk C., (2009) Donors and Users of Human Tissue for Research Purposes: Conflict of Interests and Balancing of Interests.

Rainbow C., Sought After Cells, Adapted from John Moore v. The reagents of the university of california et al. Supreme Court of California No. S006987at http://www.bio.davidson.edu/people/kabernd/Indep/carainbow/Cells.htm, accessed 29.05.2010

Tavani H. & Bottis M., The consent process in medical research involving DNA databanks: some ethical implications and challenges, ACM SIGCAS Computers and Society, vol. 40, iss. 2, June 2010, pp. 11-21

Bottis M. (2000), Comment on a view Favoring ignorance of genetic information: Confidentiality, autonomy beneficence and the right not to know EJHL 7 (2), pp. 173-183.

Mason J. et al. (2002), Law and Medical Ethics, 459, Butterworths LexisNexis, Sixth Edition, UK.

World Medical Association Declaration of Helsinki

# Protection of communications in cartel investigations

**Nikolaos E. Farantouris**

## The problem

The protection of communications between lawyers and their clients ('legal professional privilege') is the essential corollary to the client's rights of defence.[1] It is based on the specific role of the lawyer as 'collaborating in the interests of justice'[2] and as being required to provide, in full independence, and in the overriding interests of justice, such legal assistance as the client needs.[3] Lawyers would be unable to carry out satisfactorily their task of advising, defending and representing their clients, if they were obliged, in the context of judicial proceedings, to cooperate with the authorities by passing them information obtained in the course of related legal consultations.[4] However, the scope of the protection afforded by legal professional privilege has recently been disputed in the context of antitrust procedures. The question is whether and, if so, to what extent internal company communications, such as electronic mail etc., with enrolled in-house lawyers are covered by the protective scope of legal professional privilege. This paper examines, in particular, the way in which the legal professional privilege, guaranteed as a fundamental right under the law of the European Union, applies to internal exchanges of opinions and information between the management of an undertaking and an 'enrolled in-house lawyer' in cartel investigations. The scope of the protection will ultimately determine the extent of the Commission's powers of investigation in antitrust proceedings.[5]

## General legal framework

In EU law the protection of communications between lawyers and their clients has the status of a general legal principle in the nature of a fundamental right. This follows, on the one hand, from the principles common to the legal systems of the Member States:[6] legal professional privilege is currently recognised in all 27 Member States of the European Union. In some Member States this protection is enshrined in case-law alone,[7] but in most of which it is provided for at least by statute if not by the constitution itself.[8] On the other hand, the protection of legal professional privilege also derives from Article 8(1) of the ECHR (protection of correspondence) in conjunction with Article 6(1) and (3)(c) of the ECHR[9] (right to a fair trial) as well as from Article 7 of the Charter of Fundamen-

tal Rights of the European Union[10] (respect for communications) in conjunction with Article 47(1), the second sentence of Article 47(2) and Article 48(2) of that Charter (right to be advised, defended and represented, respect for rights of the defence).[11]

In AM & S,[12] the Court recognised that 'the confidentiality of written communications between lawyer and client' must also be protected at Community level (now, at European Union level). For the purposes of reliance on that protection, the Court identified two cumulative conditions ('criteria') which it had drawn from a combination of the laws of all the Member States at that time:[13] First, the communication with the lawyer must have a connection with the exercise of the client's rights of defence: it must be a 'communication' made 'for the purposes and in the interests of the client's rights of defence' (connection with the rights of defence). Second, it must be a communication with an independent lawyer, that is to say with a lawyer who is 'not bound to the client by a relationship of employment' (independence of the lawyer). More problematic appears to be the second of these criteria, i.e. the independence of the lawyer with whom communications were exchanged. In AM & S, the requirement of independence is unequivocally linked to the fact that the lawyer in question must not be in a relationship of employment with his client. The explicit reference to this fact at two points in the grounds of the judgment[14] would have been redundant if the Court had intended that the formal act of admission to a Bar or Law Society and the professional ethical obligations associated with such admission would alone be sufficient to guarantee the independence of an in-house lawyer. In AM & S, the Court, therefore, deliberately interpreted legal professional privilege as meaning that the protection which it affords does not extend to internal company or group communications with enrolled in-house lawyers. This becomes particularly apparent when the judgment is compared with the Opinion of Advocate General Sir Gordon Slynn. The Advocate General referred to the detailed discussion of the position of in-house lawyers which had taken place in that case and pronounced himself resolutely in favour of the proposition that legal professional privilege should also be granted to lawyers who are 'professionally qualified and subject to professional discipline' and are 'employed full time … in the legal departments of private undertakings'.[15] The Court did not concur with that view in its judgment in AM & S.

In the judgment above the concept of the independence of lawyers is determined not only positively – by reference to professional ethical obligations[16] – but also negatively – by reference to the absence of an employment relationship.[17] It is only where an in-house lawyer is subject, as a member of a Bar or Law Society, to the professional ethical obligations commonly applicable in the European Union and, furthermore, is not in an employment relationship with his client that com-

munications between the two are protected by legal professional privilege under EU law.

The reasoning behind this is that an enrolled in-house lawyer, despite his membership of a Bar or Law Society and the professional ethical obligations associated with such membership, does not enjoy the same degree of independence from his employer as a lawyer working in an external law firm does in relation to his clients. Consequently, an enrolled in-house lawyer is less able to deal effectively with any conflicts of interest between his professional obligations and the aims and wishes of his client than an external lawyer. Militating against the proposition that an enrolled in-house lawyer is sufficiently independent is, first, the fact that, as an employee, such a lawyer is often required to follow work-related instructions issued by his or her employer and is in any event part and parcel of the structures of the company or group by which he or she is employed. In the words of the General Court, an enrolled in-house lawyer is 'structurally, hierarchically and functionally'[18] dependent on his or her employer, whereas this is not true of an external lawyer in relation to his or her clients.

## The AKZO case

The background to this case was formed by a search (an 'investigation' or 'inspection') conducted by the European Commission, as competition authority, in February 2003 at the business premises of Akzo Nobel Chemicals Ltd (Akzo) and Akcros Chemicals Ltd (Akcros) in the United Kingdom. In the course of that search, the Commission officials took photocopies of certain documents, most notably two printouts of emails exchanged between the general manager of Akcros and a member of Akzo's in-house legal department, who was admitted as a lawyer to the Netherlands Bar. The representatives of Akzo and Akcros regarded those documents as being exempt from seizure because, in their view, they were covered by legal professional privilege.

This gave rise to a legal dispute between the two companies concerned and the Commission. Akzo and Akcros brought proceedings before the Court of First Instance (now: 'the General Court') against, on the one hand, the Commission's decision ordering the investigation and, on the other hand, the Commission's decision to place a number of disputed documents on the file. By judgment of 17 September 2007[19], the General Court dismissed the first action as inadmissible and the second action as unfounded. The General Court ruled that only communications between companies and their external lawyers are privileged and concluded that the Commission is therefore entitled to inspect communications with in-house counsel. On 30 November 2007, Akzo and Akcros together lodged an appeal against this judgment.[20] The appeal was concerned solely with the ques-

tion whether or not the two emails exchanged between an in-house lawyer and Akcros' general manager were covered by legal professional privilege. The appellants claim that the Court should set aside the judgment under appeal in so far as it rejected the claim for legal professional privilege in respect of communications with Akzo Nobel's in-house lawyer.

In her opinion, delivered on 29 April 2010, Advocate General Kokott takes the view that the protection of communications between lawyers and their clients under EU law applies solely to communications between a client and an external lawyer, and sees no reason to extend its scope to internal exchanges of opinions and information between the management of an undertaking and an in-house lawyer employed by that undertaking, even when he or she is a member of a Bar or Law Society. Her opinion rests essentially on the following two considerations:

First, in the Court of Justice's judgment in AM & S, in which the Court for the first time held that written communications containing legal advice from an external lawyer could not be seized when investigating suspected infringements of the competition rules, the concept of the independence of lawyers is determined not only positively – by reference to professional ethical obligations – but also negatively – by reference to the absence of an employment relationship. An in-house lawyer, despite his or her membership of a Bar or Law Society and the professional ethical obligations associated with such membership, does not enjoy the same degree of independence from his employer as a lawyer working in an external law firm does in relation to his or her clients, given his contractual relationships with - and economic dependence on - his or her employer. Consequently, an enrolled in-house lawyer is less able to deal effectively with any conflicts of interest between his or her professional obligations and the aims and wishes of his or her employer than an external lawyer in relation to his or her clients. Given the difference in the degree of independence between in-house lawyers and external lawyers, Advocate General Kokott also dismisses Akzo and Akcros' claims that treating in-house lawyers differently from external lawyers infringes the principle of equal treatment and non-discrimination, which is a general principle of EU law.

Secondly, Advocate General Kokott finds that there is no need to extend the scope of legal professional privilege under EU law. Whereas legal professional privilege for an external lawyer is recognised in all 27 Member States, there is no identifiable general trend in the legal systems of the 27 Member States towards extending legal professional privilege to in-house lawyers admitted to a Bar or Law Society since AM&S, nor are there overriding reasons which would require that EU law be brought in line with the legal position of a minority of Member States.

Essentially for these reasons, Advocate General Kokott proposes that the Court should dismiss the appeal. The Advocate General's opinion is certainly not bind-

ing on the Court of Justice, which must now decide on the appeal lodged by Akzo and Akros against the judgment of the General Court.

## Legal privilege and the modernisation of EU competition law

During the process of drawing up legislation to modernise European law governing antistrust proceedings (Regulation No 1/2003) and to revise the EC Merger Regulation (Regulation No 139/2004), members of the European Parliament tabled proposals aimed at extending legal professional privilege to in-house lawyers[21]. However, those proposals were ultimately not adopted by the legislature.[22] Eventually, the modernisation of the law governing antitrust proceedings carried out by Regulation No 1/2003 has led to an increasing need for internal corporate legal advice the role of which in preventing infringements of competition law is crucial.

The legal advice given by enrolled in-house lawyers in cartel investigations is particularly valuable in day-to-day business because it can be obtained more quickly and more economically and because it is based on an intimate knowledge of the undertaking concerned and its business. Moreover, there is a growing importance of 'compliance programmes' within undertakings, which serve to ensure that the undertaking conducts itself in accordance with the law and the relevant rules and regulations. The effective provision of internal corporate legal advice and a successful compliance programme are dependent on the possibility of free and faithful internal company or group communications with enrolled in-house lawyers. Otherwise, the company's management will be averse to disclosing sensitive information to an enrolled in-house lawyer and the enrolled in-house lawyer will be inclined to give advice orally rather than in writing, thus compromising the quality and usefulness of the legal advice required.

The question, however, remains whether the increased importance of enrolled in-house lawyers or the indisputable usefulness of their legal advice under the scheme of Regulation No 1/2003 supports the proposition that internal company or group communications should be placed under the protection of legal professional privilege. At this juncture, Advocated General Kokott considered that an extension of scope of legal professional privilege to in-house lawyers cannot be justified by reference to the advantages and significance of internal corporate legal advice or to the procedural-law reform carried out by Regulation No 1/2003.[23]

## Final Remarks

Both the General Court and Advocate General preferred to adopt a 'literal' interpretation of the judgment of the Court of Justice in AM & S instead of interpreting and applying it in accordance with its spirit and purpose. The question

whether an enrolled in-house lawyer is in fact able to give independent legal advice was answered by adopting an excessively formalistic approach and of losing sight of the principles underlying the criterion of independence. The objection to this approach relates to the professional and ethical obligations to which lawyers admitted to a Bar or Law Society are generally subject.[24] Due to the professional ethical obligations applicable to him or her, an in-house lawyer who is also a member of a Bar or Law Society automatically enjoys the same independence as an external lawyer who pursues his or her profession on a self-employed basis or as an employee of a law firm. The guarantees as to the independence of a qualified lawyer under many Member States' law are in fact particularly extensive. For instance, differences of opinion relating to the nature and substance of legal advice provided by an enrolled in-house lawyer do not entitle the employer to take disciplinary measures against the enrolled in-house lawyer and certainly not to terminate the employment relationship. On the other hand, external lawyers are also economically dependent to some extent on their clients, while enrolled in-house lawyers are protected against dismissal under employment law.

The opinion of Advocate General Kokott is a setback for the rights of defence. The role of the in-house lawyer has developed very considerably since the AM & S judgment 28 years ago. Today, a large number of corporations have extensive in-house legal departments staffed by highly ethical lawyers who are members of their Bar or Law Society, and whose professional obligations take precedence over their obligations to their employer. Very often such lawyers are in the front line in securing the undertaking's compliance with the law. One would have thought that it was appropriate to reinforce that role, not undermine it.

On a 'teleological interpretation' of AM & S, the Court of the EU would concluded that internal company communications with enrolled in-house lawyers in cartel investigations are covered by the protective scope of legal professional privilege. In the light of their crucial importance, the fundamental right of legal privilege must in principle be interpreted extensively. However, irrespective of Court's pending ruling in AKZO case, it is submitted that the Commission should take an ad hoc approach, by ascertaining on a case-by-case basis whether a given in-house lawyer satisfies the requirement of independence. In any case, it seems disproportionate to refuse to extend the protection afforded by legal professional privilege to internal company communications with enrolled in-house lawyers as a general principle. Information about the provisions governing the profession of lawyer in a particular Member State would itself be sufficient to make it possible to determine conclusively whether an in-house lawyer is independent or not.

## Endnotes

1. See, inter alia, Case 155/79 *AM & S v Commission* [1982] ECR 1575, in particular paragraphs 20 and 23. See also, in the case-law of the European Court of Human Rights, *André and Other v France*, No. 18603/03, 24 July 2008, paragraph 41.
2. Cf. the phrase 'collaborating in the interests of justice' used by the Court of Justice in AM & S (ibid.). A lawyer is more commonly described in German legal terminology as 'Organ der Rechtspflege' (organ of the administration of justice).
3. See, in the case-law of the European Court of Human Rights (ECtHR), *Niemietz v Germany*, 16 December 1992, Series A No. 251-B, paragraph 37.
4. Case C-305/05 Ordre des barreaux francophones et germanophone and Others [2007] ECR I-5305, paragraph 32.
5. Council Regulation 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (OJ 2003 L 1, p. 1). Regulation 1/2003 replaced Council Regulation (EEC) No 17 of 6 February 1962, the first Regulation implementing Articles 85 and 86 of the Treaty (OJ, English Special Edition 1959-1962, p. 87). On the replacement of Regulation No 17 by Regulation No 1/2003, see Article 43(1) in conjunction with Article 45 of Regulation No 1/2003.
6. See, for example, Case 155/79 *AM & S v Commission* [1982] ECR 1575, in particular paragraph 18. See also the Opinion of Advocate General Léger in Case C-309/99 Wouters and Others [2002] ECR I-1577, point 182; and the Opinion of Advocate General Poiares Maduro in Ordre des barreaux francophones et germanophone and Others [2007] ECR I-5305, point 39. In addition, see the Order in Case T-30/89 *Hilti v Commission* [1990] ECR II-163, paragraphs 13 and 14.
7. I.e. in the United Kingdom and Ireland.
8. Legal professional privilege is enshrined in constitutional law in particular in Bulgaria (Article 30(5) of the Bulgarian Constitution) and Spain (Article 24(2) of the Spanish Constitution). Furthermore, legal professional privilege is also based on constitutional provisions in Italy, Portugal and Romania, among others, and on statutory provisions with the status of constitutional law in Sweden; Case C-550/07, *Akzo Nobel Chemicals Ltd and Akros Chemicals Ltd v Commission*, per Advocate General Kokott, 29 April 2010, fn. 34.
9. The case-law of the European Court of Human Rights (ECtHR) usually refers only to Article 8 of the ECHR; in this regard, see, for example, *Campbell v UK*, 25 March 1992, Series A No. 233; Niemietz v Germany, 16 December 1992, Series A No. 251-B; Foxley v UK, No. 33274/96, 20 September 2000; *Smirnov v Russia*, No. 71362/01, 7 June 2007, ECHR 2007-VII; and *André and Other v France*, No. 18603/03, 24 July 2008. However, mention is sometimes also made of Article 6 of the ECHR (see, for example, *Niemietz v Germany*, op. cit., § 37, and *Foxley v UK*, op. cit., § 50).
10. The Charter of Fundamental Rights of the European Union was solemnly proclaimed first in Nice on 7 December 2000 (OJ 2000 C 364, p. 1) and then again in Strasbourg on 12 December 2007 (OJ 2007 C 303, p. 1).
11. See, inter alia, Case C-432/05 Unibet [2007] ECR I-2271, paragraph 37; Case C-540/03 Parliament v Council [2006] ECR I-5769, paragraph 38; and point 108 AG's Opinion in

Case C-550/07, *Akzo Nobel Chemicals Ltd and Akros Chemicals Ltd v Commission*, per Advocate General, 29 April 2010.

12. Case 155/79 AM & S v Commission [1982] ECR 1575.
13. Ibid, paragraphs 21 and 22.
14. Ibid, paragraphs 21 and 27.
15. Opinion of Advocate General Sir Gordon Slynn in AM & S (ibid.) at p. 1655.
16. AM & S (ibid.), paragraph 24.
17. Ibid., paragraphs 21 and 27. See also the Opinion of Advocate General Léger in Case C-309/99 *Wouters and Others* [2002] ECR I-1577, point 181: '[The independence of lawyers] must also be demonstrated vis-à-vis the client, who may not become his lawyer's employer.'
18. Joined Cases T-125/03 and T-253/03 *Akzo Nobel Chemicals and Akcros Chemicals v Commission* [2007] ECR II-3523, paragraph 168.
19. Ibid.
20. Case C-550/07, *Akzo Nobel Chemicals Ltd and Akros Chemicals Ltd v Commission*.
21. With regard to Regulation No 1/2003, see Parliamentary Document A5-0229/2001 final (Evans Report), specifically Amendment 10 relating to Article 14(3) of the Commission's proposal for a regulation COM(2000) 582 final; with regard to Regulation No 139/2004, see Parliamentary Document A5-0257/2003 final (Della Vedova Report), specifically Amendment 5 relating to the 34th recital and Amendment 25 relating to Article 13(1) of the Commission's proposal for a regulation COM(2002) 711 final.
22. In the case of Regulation No 1/2003, the Parliament as a whole did not itself support the amendments proposed by its own members. With regard to Regulation No 139/2004, while the amendments were approved by the Parliament, the Council did not include them in the Regulation.
23. The Commission's powers of investigation in reviewing mergers of European companies under Article 13 of Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation, OJ 2004 L 24, p. 1) are similar to, and only slightly less extensive than, those under Article 20 of Regulation No 1/2003.
24. See, e.g. in Greece, articles 38, 39 62 and 63(3) and (4) of the Lawyers' Code of Conduct, and article 94 of the Code of Civil Procedure; cf. Decision of the Athens Court of Appeal 1466/2003. Ireland goes further than this, in that it seems to want to extend the protection afforded by legal professional privilege even to in-house lawyers whose 'independence' is guaranteed by provisions of employment law alone (paragraph 12 of the statement in intervention in Case C-550/07, *Akzo Nobel Chemicals Ltd and Akros Chemicals Ltd v Commission*.

## References

Brüssow, R., Das Anwaltsprivileg des Syndikus im Wirtschaftsstrafverfahren, in: Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltvereins [ed.], Strafverteidigung im Rechtsstaat, Baden-Baden 2009, p. 91-106

Cheynel, B., Heurs et malheurs du "legal privilege" devant les juridictions communautaires, Revue Lamy de la Concurrence – Droit, Économie, Régulation 2008, No 14, p. 89-93

Gray, M., The Akzo Nobel Judgment of the Court of First Instance, Irish Journal of European Law 14 (2007), p. 229-242

Huff, M., Recht und Spiel, in: Frankfurter Allgemeine Zeitung No 183, 10 August 2009, p. 28

Mykolaitis, D., Developments of Legal Professional Privilege under the Akzo/Akcros Judgment, International Trade Law and Regulation 2008, p. 1-6

Prieto, C., Pouvoirs de vérification de la Commission et protection de la confidentialité des communications entre avocats et clients, La semaine juridique – édition générale 2007, II-10201, p. 35-37

Weiß, W., Neues zum legal professional privilege, Europarecht 2008, p. 546-557

# Web accessibility guidelines: the debate over enforcement

**Andreas Giannakoulopoulos**

## Web Accessibility: Definition and History

Web accessibility refers to "the ease of use of information and communication technologies (ICTs), such as the Internet, by people with disabilities" [World Health Organization, 2010]. When sites are correctly designed, developed and edited, all users can understand, interact with and contribute to the web. Based on this fundamental principle, Tim Berners-Lee, an MIT professor credited with inventing the World Wide Web in early '90s, formed, in 1994, the World Wide Web Consortium; a body responsible for coordinating the development of web standards. Its declared aim was actually to create standards to improve the quality of the web.

In the same year, the first meeting of the W3C Advisory Committee took place. Its aim was stated as follows:

"The World Wide Web Consortium (W3C) develops interoperable technologies (specifications, guidelines, software, and tools) to lead the web to its full potential." [World Wide Web Consortium, 1994]. The World Wide Web Consortium decided that its standards should be based on royalty-free technology, so that they could be freely and easily adopted by anyone. Currently the W3C has 333 member organizations from over 30 countries [World Wide Web Consortium, 2010].

Another landmark in the very recent history of web accessibility is 1997, the year that the W3C introduced the Web Accessibility Initiative (WAI). The WAI is a W3C group responsible for developing guidelines which will ensure web resources are widely accessible. Its aim was to address the question of how to expand access to the web for people with disabilities.

Two years later, the W3C published the first official Recommendation on accessibility issues, namely Web Content Accessibility Guidelines 1.0. [World Wide Web Consortium, 1999]. Its aim was to help web content developers understand how to make their content more accessible to a wide audience (not only disabled people).

In 2008 the W3C developed and published Web Accessibility Guidelines 2.0, an improved version of WCAG 1.0 which, too, became an official Recommendation [World Wide Web Consortium, 2008].

## Web Content Accessibility Guidelines

### *Technical Description*

Web Content Accessibility Guidelines are one of a series of guidelines published by the Web Accessibility Initiative with the purpose of providing advice for making web content accessible, primarily for disabled users, but also for all users and all user agents, including highly limited devices, like mobile phones. Other sets of WAI guidelines, like User Agent Accessibility Guidelines (UAAG) and Authoring Tools Accessibility Guidelines (ATAG) cover accessible user agents (browsers) and accessible authoring tools [World Wide Web Consortium, 1999].

In May of 1999, WAI published its first set of Web Content Accessibility Guidelines, WCAG 1.0. WCAG 1.0 was a step toward standardizing accessibility; as stated by the World Wide Web Consortium, WCAG 1.0 consists of the following 14 guidelines which entail 3 testable priority levels/success criteria:

Fourteen guidelines

1. Provide equivalent alternatives to auditory and visual content.
2. Don't rely on color alone.
3. Use markup and style sheets and do so properly.
4. Clarify natural language usage.
5. Create tables that transform gracefully.
6. Ensure that pages featuring new technologies transform gracefully.
7. Ensure user control of time-sensitive content changes.
8. Ensure direct accessibility of embedded user interfaces.
9. Design for device-independence.
10. Use interim solutions.
11. Use W3C technologies and guidelines.
12. Provide context and orientation information.
13. Provide clear navigation mechanisms.
14. Ensure that documents are clear and simple.

Three Priority Levels

Priority 1: A web content developer must satisfy this checkpoint. Otherwise, one or more groups will find it impossible to access information in the document. Satisfying this checkpoint is a basic requirement for some groups to be able to use web documents.

Conformance to this level is described as A.

Priority 2: A web content developer should satisfy this checkpoint. Otherwise, one or more groups will find it difficult to access information in the document. Satisfying this checkpoint will remove significant barriers to accessing web documents.

Conformance to this level is described as AA or Double-A.

Priority 3: A web content developer may address this checkpoint. Otherwise, one or more groups will find it somewhat difficult to access information in the document. Satisfying this checkpoint will improve access to web documents.

Conformance to this level is described as AAA or Triple-A. [World Wide Web Consortium, 1999].

However, WCAG 1.0 underwent much criticism. First, it applied mostly to HTML format. Its critics wanted guidelines that could be applied to broader technologies and that could also be applied to future technologies. Furthermore, a number of WCAG 1.0 guidelines were considered out-of-date. [Piacello, 2000]. Some of the out-dated guidelines include:

- Provide equivalent text links for links within client-side image maps.
- Provide abbreviations for table header labels, if you use these.
- Use access keys (keyboard shortcuts) for important links.
- Don't use tables with more than one column for layout.
- Make sure form fields aren't empty by default.
- Ensure different links have non-link text between them.

WAI responded in 2006 with WCAG 2.0. This second version of WCAG was an attempt to make the guidelines more robust, measurable, and technology-independent. Unlike WCAG 1.0, WCAG 2.0 provides a list of common failures and offers some examples of common errors. The other major improvement in this document is that the examples provided are far more realistic. Furthermore, a number of new guidelines have been brought into WCAG 2.0. Some of these guidelines are totally new whereas others were hinted at, but not specifically stated, in WCAG 1.0. Some examples include:

- Providing text-based error messages for forms
- Ensure all pages have a descriptive title
- Background noise can be turned off [Moss, 2006].

This revised version of the accessibility guidelines begins with a set of four principles necessary for content to be accessible. Content must be perceivable, operable, understandable, and robust. Accompanying those principles are twelve guidelines which serve as general goals for developers. According to the WAI website, those four principles and twelve guidelines are:

Principle 1: Perceivable - Information and user interface components must be presentable to users in ways they can perceive.

Guideline 1.1 Text Alternatives: Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language.

Guideline 1.2 Time-based Media: Provide alternatives for time-based media.

Guideline 1.3 Adaptable: Create content that can be presented in different ways (for example simpler layout) without losing information or structure.

Guideline 1.4 Distinguishable: Make it easier for users to see and hear content including separating foreground from background.

Principle 2: Operable - User interface components and navigation must be operable.

Guideline 2.1 Keyboard Accessible: Make all functionality available from a keyboard.

Guideline 2.2 Enough Time: Provide users enough time to read and use content.

Guideline 2.3 Seizures: Do not design content in a way that is known to cause seizures.

Guideline 2.4 Navigable: Provide ways to help users navigate, find content, and determine where they are.

Principle 3: Understandable - Information and the operation of user interface must be understandable.

Guideline 3.1 Readable: Make text content readable and understandable.

Guideline 3.2 Predictable: Make web pages appear and operate in predictable ways.

Guideline 3.3 Input Assistance: Help users avoid and correct mistakes.

Principle 4: Robust - Content must be robust enough that it can be interpreted reliably by a wide variety of user agents, including assistive technologies.

Guideline 4.1 Compatible: Maximize compatibility with current and future user agents, including assistive technologies. [Web Accessibility Initiative, 2008]

In order to ensure accessibility, each of these principles and guidelines must be in place. The guidelines are further broken down into criteria which provide specific instructions, and developers can test accessibility using these criteria. The WCAG 2.0 also provides a number of techniques, examples of proper content accommodations and common failures. WAI categorizes conformance into one of three levels with A being the lowest, AA the next higher, and AAA being the highest. However, it is possible for some websites to meet AAA criteria level, and still have accessibility issues [Clark, 2006], a fact that strengthens the argumentation against accessibility guidelines enforcement, as will be pointed out further on in this paper.

WCAG 2.0 promised to be the new touchstone. Its first installment, however, was again met with much critique. Comparing WCAG 1.0 and WCAG 2.0, some points had been simplified in 2.0 but in some cases the points in the second version were more complex than those in the first. The documents themselves were lengthy and wordy, filled with jargon and clearly not all too accessible [Moss, 2006]. Critics argued that WCAG 2.0 was very difficult to comply with and that it did not even include the most rudimentary demands of valid HTML. Those remarks raised doubt as to whether WCAG 2.0 could actually achieve its primary function –improving web accessibility by providing clear, practical (i.e. real-world), and achievable standards for creating websites and content [Sundell, 2006]; as will be discussed in more detail later on, such criticism adds a rather big arrow, so to speak, in the quiver of those opposing the enforcement of accessibility guidelines.

## *Basic Principles-Directions*

As the Web Accessibility Initiative notes, "the web is an increasingly important resource in many aspects of life; education, employment, government, commerce, health care, recreation and more. [Web Accessibility Initiative, 1994]. Recognizing that disabled people have a right to participate in all walks of life and the importance of accessibility to the cultural environment and to information and communication, the UN Convention on The Rights of Persons with Disabilities provides a recognized international standard for disabled people's human rights. 82 countries signed the convention on the 30th of March 2007. Since then, nearly 140 more countries have signed it, with almost 60 having ratified [United Nations, 2007].

Moreover, the web is essentially a place of interaction, and especially for disabled people, the set-up of a particular website may prevent full interaction. Both accessibility and ability are usually taken for granted, but it would be worth considering the example of a website requiring the use of a mouse and how impossible a task that would be for someone with a physical disability limiting hand movement. Or maybe a website is not providing text in place of important images, so a person with low or no vision is not fully experiencing the content as intended. It is essential that the web be accessible in order to provide equal access and equal opportunity to people with disabilities. An accessible web can also help people with disabilities more actively participate in society [European Commission, 2010].

Both WCAG 1.0 and 2.0 were designed so that "people with disabilities can perceive, understand, navigate, and interact with the web, and that they can contribute to the web" [Web Accessibility Initiative]. This, in short, is the basic principle behind the creation of web accessibility standards and the effort to disseminate those standards to web content developers and raise concern for accessibility issues in general.

## Stakeholders-Beneficiaries

Crucial to the ongoing debate over enforcement of web accessibility guidelines is the question of who those guidelines actually concern, in other words, who benefits from the enhancement of web content access and the enforcement of standards on web content developers. As will be shown, accessibility guidelines compliance is in the advantage of a much wider audience than one might initially think.

It is a fact that around 10 per cent of the world's population, or 750 million people, live with a disability. They are the world's largest minority. This figure is increasing through population growth, medical advances and the ageing process, says the World Health Organization (WHO) [United Nations, 2010].

However, web accessibility is a requirement concerning not only congenitally disabled people, but also people operating under permanent or temporary constraints, in general (physical constraints or special conditions). More specifically, users who benefit from accessibility guidelines compliance are not only people disabled at birth, but also those who have suffered some type of injury, people facing the problems of ageing and, finally, people without any form of disability whatsoever, i.e. users with different needs and preferences and people working under special constraints (e.g. slow Internet connection, noisy, over-illuminated or hands-free environment). All of the above, indicatively and not exclusively, might have physical, sensory cognitive disabilities or other constraints affecting web content access.

It is obvious, then, that everyone benefits from widespread awareness of web accessibility issues as well as the related good practices, since it is very likely that almost every one of us will someday have to face the predicaments of ageing or some other kind of constraint to free and easy web access.

## Methods of Evaluation

Another important part of the argumentation concerning accessibility guidelines enforcement is related to the methods of evaluating compliance to web accessibility standards and their disputed adequacy and efficiency.

Web accessibility evaluation can be objective and automated with the use of specific tools that is, software programs or online services, like Bobby, RAMP, InFocus, A-Prompt, and LIFT which help find accessibility flaws in websites before the sites are publicly posted [Ivory, Mankoff and Le, 2003]; they can also be subjective and manual, involving human judgement (by specialists or, where necessary, with the participation of members of the specific group the web content is addressing). Evaluation of accessibility can also be semi-automated, i.e. combining the use of automatic evaluation tools and human assessment. Since accessibility tools can only partially check accessibility through automation, the combined use of automated tools and human judgement is the most reliable means of determining whether web content is accessible or not.

An important classification of automated software tools is their cost. There are a number of free evaluation tools, but there are also cases when specific needs have to be addressed and a commercially available tool may be preferable. The cost of an evaluation tool greatly depends on the accessibility knowledge of its user. Free tools often assume a greater understanding and spend less time educating their user. Commercially available tools are also more time-saving –they do not have to check a site one page at a time, as it happens with free tools which have a more limited scope– and they often produce more detailed and specific reports.

Furthermore, another classification of accessibility evaluation tools involves where these tools are meant to function. Some tools are available at a website where developers can evaluate the content of a page quickly and easily without downloading or installing an application. Other options include tools that are created as extensions to a browser, tools that function as part of a web authoring tool, whereas some tools require installation on a hard drive or server, like other pieces of software.

Finally, evaluation tools can be classified according to their repair functionality. Many tools can only perform an evaluation, but some tools are able to perform the evaluation and guide the repair process. This is a more common characteristic

of commercially available tools. These often spend time educating their user and guiding both the evaluation and repair process [WebAim, 2010].

## Arguments In Favor of WCAG Enforcement

### *People-Oriented Arguments*

Supporters of the enforcement of web accessibility guidelines put forth a number of reasons why such enforcement is beneficial to all users. As we have already argued, web accessibility is/should be everyone's concern, since disabled people constitute a considerable part of the world's population and, at the same time, a mere part of a much wider audience, consisting of people having or being bound to have some kind of constraint to free and easy access to web content.

More specifically, as the World Health Organization estimates, between 750 million and 1 billion of the world's 6 billion people have a speech, vision, mobility, hearing or cognitive impairment and, as stated in the UN Convention on the Rights of Persons with Disabilities, web access is a basic human right, not a privilege. Having entered the knowledge society, in which new technologies constitute a sine qua non, and having acknowledged the socio-political value of the web, and most importantly, its power to promote democracy, we cannot but recognize everybody's right to free and easy web access. Obviously enough, however, compliance to the guidelines also affects people with temporary ailments, seniors and practically any user, since everyone benefits from a coherent, consistent and functional web [Giannakoulopoulos, 2005].

Moreover, enforcing accessibility guidelines is also a means for a state to provide active support to disabled people. For a modern state, Internet is nothing less than basic infrastructure. Its way of exhibiting real concern for its disabled citizens is enforcing legislation that guarantees the deployment of WCA guidelines. Enhancing web accessibility is a state responsibility and it cannot be left on pure chance or the good will of web content developers.

Enforcement also ensures that organizations which would otherwise ignore matters of web accessibility conform to the guidelines for fear of non-compliance sanctions. Experience has shown that if there is no legal obligation, there is probably no concern for accessibility issues, either. Social responsibility is just a lofty ideal and, simply put, the stick could prove far more effective than the carrot [Budd, 2005]

### *Output-Oriented Arguments*

The argumentation in favor of web accessibility guidelines enforcement is also built on the assumption that enforcement achieves enhancement of web coher-

ence/functionality and promotes its fundamental feature –universality (The Web is World Wide, after all). There is a pressing need for the internationalization of the web, so it is important to disseminate best practices and standards related to managing web content. Standards enable interoperability of data and encourage coherence across the web.

Further, conformity to regulations and standards leads to uniformity ("write once, read everywhere"), i.e. reduces variety and prevents fragmentation, brought about by different approaches to accessibility issues. Standardization ensures measurable results, as well as consistency, credibility and comparability.

Finally, when accessibility guidelines are enforced, it is ensured that companies will address a wider audience and a whole new market; all people with disabilities [Clark, 2002].

## Arguments Against WCAG Enforcement

### *People-Oriented Arguments*

In the debate over WCAG enforcement, as the only means that could guarantee the enhancement of web accessibility, those opposing it emphasize the predominant role of the "agent" (web designer, developer or evaluator) in achieving accessibility, highlighting the importance of guidelines maintaining their assistive character; simply put, providing guidelines should merely mean "helping". The very essence of the word "guideline" is irrelevant to laws, rules and regulations. Guidelines entail the idea of providing assistance to web content developers to achieve accessibility and not impose a certain way of achieving it. The guidelines should presume that developers are trying to make web content accessible and the latter should be given the freedom to choose (even choose wrong).

More importantly, education of developers, clients and suppliers could guarantee a widespread sensitivity to accessibility issues and, thus, should be prioritized and not underestimated. It follows, then, that a combination of good tools, improved practice and education are much better alternatives and should be given priority against a "regulations mindset".

### *Output-Oriented Arguments*

Seen from a purely practical viewpoint, WCAG enforcement seems to be rejected by some as almost idealistic. One cannot but pose the question of what exactly should be enforced, since there is an ongoing search of standards. The web content development industry is an immature one; guidelines are in development and their interpretation changes constantly. Further supporting the claim about the insufficiency of guidelines, some point to the absence of a common agreement among

experts on web accessibility standards, which, it should be noted, are not developed via collaborative processes; each government could adopt a different technical standard based on new, conflicting guidelines. A survey in the UK and Oman has shown that no matter what tools are used or how logically the site is designed, if the designer has not fully understood the culture and the client's market, the site is unlikely to succeed. [Beirekdar, Vanderdonckt & Noirhomme-Fraiture, 2002].

Apart from the "relativity" issue, though, there is always the huge problem of evaluation. Some semi-automated tools for measuring compliance with the guidelines are strongly criticized as insufficient; their output is unfriendly and they often flag nonexistent accessibility problems. Despite the advantages of automated evaluation, there is little evidence about their efficacy; specifically, if they result in better sites than those produced without tools and if they actually result in more accessible, usable web content. [Ivory, Mankoff & Le, 2003].

Further, there are several important aspects of accessible web page design than cannot yet be tested by automated tools, because they need human assessment. When subjective/manual evaluation comes into play, there is naturally ample room for dispute. More importantly, web content that does not meet the standards runs the risk of potential loss of business by being "named and shamed" by pressure groups. Not surprisingly, evaluation could very easily run the risk of being manipulated to serve specific interests.

Further arguing against web content accessibility guidelines enforcement, those opposing it emphasize the importance of motivation as a more successful means of achieving the dissemination of web content accessibility standards and guidelines amongst web content developers. It is important to examine how the carrot could prove more effective than the stick, so to speak, as far as raising awareness of accessibility issues is concerned.

Interestingly, the fear of the strong arm of the law is not a strong motive. E.g. in Australia, the last sue against a major Organization (Maguire vs. Sydney Organizing Committee for the Olympic Games) was in 2000 [Australian Human Rights Commission, 2000]. Given that tools and guidelines are available to help in building accessible websites, and given that public policy generally supports web accessibility, research has shown that, surprisingly, many websites remain inaccessible [Travis, 2004].

As Thain points out, intrinsic motives could prove more effective and enforcement should be a last resort. Rather than berating web content developers for non-compliance with accessibility guidelines, they should be encouraged towards appreciating, first, the positive aspects/benefits of proper web authoring, namely:

a) positive PR that comes from adopting a socially responsible attitude,

b) ability to address a wider audience and

c) the fact that accessible sites are inherently more search engine friendly.

At the same time, emphasis should also be put on the negative aspects of inaccessibility: turning away of a large number of potential users and bad publicity. Common experience has shown that people are more likely to share a negative experience of a website than a positive one. Consequently, denying access of web content even to a few people could generate negative PR [Thain, 2009].

## Current Examples

### *National/International Policies*

One of the first initiatives to promote accessibility was The United Nations World Program of Action (adopted in December 1982). The action program sought the equalization of opportunities for persons with disabilities and mandated that access to information and communication be a human right.

The Convention on the Rights of Persons with Disabilities and its Optional Protocol was adopted in December 2006. There were 82 signatories to the Convention, 44 signatories to the Optional Protocol, and one ratification of the Convention. It is now signed by 146 countries, ratified by 88.

On the fundamental issue of accessibility (Article 9), the Convention requires countries to identify and eliminate obstacles and barriers and ensure that persons with disabilities can access information and communications technologies [United Nations, 2006].

As far as Europe is concerned, it is important to note that the European Union cofunded the development of the W3C's Web Accessibility Guidelines. In December 2008, the European Commission published a Communication to the European Parliament, the Ministers' Council, the Economic and Social European Committee and the Lands' Committees:

"Towards an accessible information society". This communication states:

"As our society is evolving to an 'information society', we are becoming intrinsically more dependent on technology-based products and services in our daily lives. Yet poor e-accessibility means many Europeans with a disability are still unable to access the benefits of the information society.

The Commission considers it is now urgent to achieve a more coherent, common and effective approach to e-accessibility, in particular web accessibility, to hasten the advent of an accessible information society" [European Commission, 2008].

Further, the Treaty of Lisbon (2009) recognized that special attention should be given to disabled people and the fight against "info-exclusion". The European Commission has for itself carried out in the summer of 2009 an evaluation of the accessibility of its websites [European Commission, 2009].

The very recent developments in Finland, the first country in the world to make broadband a legal right for every citizen, should also be mentioned; by July 1st, 2010 all telecommunications companies are obliged to provide all residents with broadband lines. It is believed that up to 96% of the population are already online and that only about 4,000 homes still need connecting to comply with the law [Guardian, 2009].

In the case of the U.S.A., Section 508 was enacted in 1998 to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals. Section 508 Standard of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency [United States Government, 1998].

U.S. Section 508 was based on the W3C WCAG 1.0 version. Rather than adopt the WCAG standard directly, the U.S. created a separate legislation. The majority of web Section 508 rules are based on Priority Level 1 of the W3C WCAG but there are some rules that are additional to the WCAG guidelines [Mueller, 2003].

Noteworthy are also the cases of Australia and Canada, the former expanding WCAG conformance to commercial websites and the latter requiring WCAG conformance level AA which is a rather strict requirement.

### *Organizational Policies (business case)*

Moving on to the current status as far as organizational policies are concerned, it is obvious that these days, as more and more facets of our lives become tied to Internet technologies, there is a widespread awareness of web access issues and those involved with the placement of information on the Internet cannot but consider the obstacles faced online by individuals with disabilities and design with those obstacles in mind. Across the globe, there are now public policies and laws protecting the rights of people with disabilities to access the content of the web.

The legal framework put in place by, as we have seen, several countries to ensure equal access to governmental services, has driven a movement towards making information technology products more accessible.

While Section 508, for instance, was written for federal agencies, it had a broad impact on companies that sell IT systems to the federal government. Section 508 applies to all IT systems purchased by the federal government, including PCs, software and office equipment such as copiers and fax machines. Information technology companies all over the world are also putting in a lot of effort to ensure that their products conform to necessary accessibility standards. Moreover, as Gokhale remarks, "in areas where treaties do not exist, there is technical guidance that may be useful. One example is the Industry Code by Australian Banker's Association (ABA) and its Industry Standards for Accessibility of Electronic Banking" [Gokhale, 2008].

## Discussion

It is true that disability policies and laws have considerably evolved over last few decades to focus on rehabilitation, education and 'mainstreaming' of people with disabilities particularly with regard to access to technologies [Gokhale, 2008].

However, as pointed out earlier on in this paper, web accessibility does not concern disabled people only. It is a much wider issue and at a fundamental level affects all users; that given, it is important that web accessibility awareness is widespread. Moreover, it is strongly argued that in order to work on the internationalization of the web, it is important to raise awareness of best practices and standards related to managing web content. Standards are believed to enable interoperability of data, to enhance coherence across the web and maximize the potential for access to information. The enforcement of standards is, for some, the only way to guarantee adherence to web accessibility principles. No real result is yielded if there is no legal obligation. Reality, though, is quite disappointing as far as the results of guidelines enforcement are concerned. The laws don't seem to be changing attitudes and behavior. Although the World Wide Web has become a predominant means of communicating and presenting information on a broad scale and to a wide audience, unfortunately website usability and accessibility continue to be a pressing problem. An estimated 90% of sites provide inadequate usability (Forrester Research 1999), and an estimated 66% of sites are inaccessible to users with disabilities (Jackson-Sanborn et al. 2002 see also Botttis 2006). There may be numerous assistive devices, such as screen readers and special keyboards, facilitating use of websites, but these devices may not improve a user's ability to find information, purchase products and complete other tasks on sites. Moreover, many webmasters' perceptions do not seem to be changing fast;

they may support the concept of web accessibility, but they cite roadblocks to accessibility such as lack of time, lack of training, lack of managerial support, lack of client support, inadequate software tools, and confusing accessibility guidelines. [Lazar, Dudley-Sponaugle & Greenidge, 2004]. Does this attitude call for guidelines enforcement?

It would be worthwhile to provide an example of the limited powers of such enforcement:

In 2004, the Disability Rights Commission (DRC) in the UK examined 1,000 UK website home pages and measured how accessible they are to disabled people. To do so, the researchers used a standard set of guidelines from the W3C's Web Accessibility Initiative (WCAG 1.0). Less than 1 in 5 websites met the most basic accessibility requirements (conformance level "A"), and just a very small fraction (0.2%) were WCAG "AA" compliant [Travis, 2004]. It remains to be answered whether these facts call for stronger enforcement, whether some web developer should be made an example of, or simply whether WCAG are poorly/ambiguously defined...

Admittedly, both versions of WAI WCAG have undergone much criticism owing to their moderate technical sufficiency. The required tasks aiming at accessibility were often seen as overwhelming and intimidating [Clark, 2006]. WAI guidelines have been criticized for the abundance of jargon, the complexity of the language used, the limited usability (e.g. the text was full of links and rather difficult to read) and WCAG 2.0, in particular, to avoid becoming obsolete, seems technology-neutral and rather vague.

However, does accessibility ultimately mean "standards compliance"? What is more important? Creating web content that is fully accessible for people with disabilities or web content that complies with local or national standards? It is questions like these that have fueled the ongoing debate over WCAG enforcement. For instance, many sites are given "WAI compliance level AAA", but it is questionable whether these claims are correct and whether the assessed sites are actually accessible. On the other hand, suppose that a site uses PDFs and that the web pages are not technically valid, the website (probably) is not even WCAG level A compliant; does this necessarily mean that it is inaccessible? One would be surprised to find that accessible web content is often non-compliant to standards and does not satisfy any legal requirements.

## Conclusions

Regrettably, enforcement has not made web content more accessible, as real-life experience has shown. Current websites, as research has shown, are three

times harder to use for people with disabilities than for users without disabilities. Moreover, current sites are twice as difficult for people older than 65 years to use than for younger users [Slatin & Rush, 2003]. Many are those who argue that education and widespread awareness of accessibility issues could yield more results as far as guidelines compliance is concerned.

Moreover, guidelines should be better viewed as "helping" tools, subject to assessment and constant improvement, not as indisputable laws. They may be a good basis, but they should better be seen as a continuum, a step in the way, not as a final destination [Zeldman, 2003]. Legal standardization could also be seen as a tool to measure accessibility and not as an intimidating means of ensuring guidelines compliance. Not aiming at punishment, standardization in the form of a strong recommendation could be gradually promoted in the public sector to yield minimal compliance to accessibility guidelines.

Seemingly, the question of whether the carrot (motivation) is preferable to the stick (fear of non-compliance sanctions) remains to be answered. Nevertheless, considering the value of knowledge and education in all aspects of life, perhaps raising sensitivity to accessibility issues and awareness about benefits, i.e. positive outcomes, from adopting an accessibility-friendly attitude, as well as negative aspects of inaccessibility, (in other words, providing motivation), could prove a more successful means of disseminating accessibility principles and standards.

Working on accessibility based on common sense, avoiding "regulations mindsets" and accepting the relativity of the "design for all" motto might be more effective in the long run; "design for most" is probably the highest possible to achieve, whereas the reality today is "design for some". Emphasis on the (cyber) ethical problematic of dealing with web accessibility issues in the modern, civilized world of acknowledged human rights, as well as on the practical benefits of making web content accessible to a wider audience of users-consumers, could, in the long run, raise hope of achieving a more accessible, functional and interoperable web for all.

## References

Australian Human Rights Commission, Bruce Lindsay Maguire v Sydney Organizing Committee for the Olympic Games, online at http://www.hreoc.gov.au/disability_rights/decisions/comdec/2000/DD000120.htm/ accessed 03/06/2010.

Beirekdar, A., Vanderdonckt, J. and Noirhomme-Fraiture, M. (2002), A Framework and a Language for Usability Automatic Evaluation of Websites by Static Analysis of HTML Source Code. In Proc. of 4th Int. Conf. on Computer-Aided Design of User Interfaces CADUI'2002 (Valenciennes, 15-17 May 2002). Kluwer Academics Pub., 337–348.

Bottis M., Access to information for people with disabilities, Ionian Law Review, 2006, pp. 34-48 (in Greek)

Budd, A. articles on Accessibility and Web Standards, Blogography, blog, online at http://www.andybudd.com accessed 03/06/2010.

Clark, J. (2002), Building Accessible Websites. Indianapolis: New Riders Publishing.

Clark, J. (2006), To Hell with WCAG 2, online at http://www.alistapart.com/topics/topic/accessibility/ accessed 03/06/2010.

European Commission, eInclusion & eAccessibility – Design for all, online at http://ec.europa.eu/information_society/activities/einclusion/policy/accessibility/dfa/index_en.htm accessed 03/06/2010.

European Commission, Information Providers Guide, The EU Internet Handbook, online at http://ec.europa.eu/ipg/standards/accessibility/index_en.htm/ accessed 03/06/2010.

European Commission (2008), Towards an accessible information society, online at http://eur-lex.europa.eu/ accessed 03/06/2010.

Giannakoulopoulos, A. (2005), Social Applications of the Internet: the problem of accessibility and the seniors.gr experiment, PhD thesis, Athens: University of Athens.

Gokhale, C., 'Web Accessibility: Overview of Laws and Guidelines', Infosys Microsoft Alliance and Solutions blog, at http://www.infosysblogs.com/microsoft/2008/04/web_accessibility_overview_of.html/ accessed 03/06/2010.

Guardian.co.uk, "Finland makes broadband access a legal right", online at http://www.guardian.co.uk/technology/2009/oct/14/finland-broadband/ accessed 03/06 2010.

Harper, S., Yesilada, Y., "Web accessibility and guidelines", Web Accessibility: A Foundation for Research, Human-Computer Interaction Series, Harper-Yesilada (Eds), Springer-Verlag, London, 2008.

Ivory, M., Mankoff, J., & Le, A. (2003), 'Using automated tools to improve website usage by users with diverse abilities'. IT and Society, 1(3), 195-236.

Jackson-Sanborn, E., Odess-Harnish, K., and Warren N. (2002). Website accessibility: A study of ADA Compliance, cited in Lazar, Dudley-Sponaugle & Greenidge, 'Improving web accessibility: a study of webmaster perceptions', (2004).

Lazar, J., Dudley-Sponaugle, A., Greenidge, KD. (March 2004), 'Improving web accessibility: a study of webmaster perceptions', Computers in Human Behavior, 20(2), 269-288.

Moss, T., "WCAG 2.0: The new W3C accessibility guidelines evaluated", online at http://www.webcredible.co.uk/user-friendly-resources/web-accessibility/wcag-guidelines-20.shtml/ accessed 03/06/2010.

Mueller, JP. (2003), Accessibility for everybody: understanding the Section 508 accessibility requirements. Berkeley: Apress.

Piacello, M. (2000), Web Accessibility for People with Disabilities. New York: CPM Books.

Slatin, J. & Rush S. (2003), Maximum Accessibility. Boston: Addison-Wesley.

Sundell, S. (2006), 'Are Web Accessibility Standards Doomed? WCAG 2.0 Eviscerated', online at http://www.spencersundell.com/blog/2006/06/01/are_web_accessibility_standards_doomed_wcag_20_eviscerated/ accessed 03/06/2010.

Thain, L., 'The Business Case for Web Accessibility', online at http://message.hitchcock.screen-play.net/the-business-case-for-web-accessibility/ accessed 03/06/2010.

Travis, D. (2004), 'Web Accessibility: No More Mr. Nice Guy', online at http://www.userfocus.co.uk/articles/drc_report.html accessed 03/06/2010.

United Nations, e-nable, website, Convention on the Rights of Persons with Disabilities, online at http://www.un.org/disabilities/convention/conventionfull.shtml/ accessed June 2010.

United States Government, Section508.gov, website, online at http://www.section508.gov/ accessed 03/06/2010.

WebAim, website, Accessibility Evaluation Tools, at http://webaim.org/articles/tools/accessed June 2010/ accessed 03/06/2010.

World Health Organization, Health Topics, Disabilities, online at http://www.who.int/topics/disabilities/en/ accessed 03/06/2010.

World Wide Web Consortium, Web Accessibility Initiative, http://www.w3.org/WAI/ accessed 03/06/2010.

World Wide Web Consortium, Web Content Accessibility Guidelines 1.0, http://www.w3.org/TR/WCAG10 accessed 03/06/2010.

Zeldman, J. (2003), Designing with Web Standards. Indianapolis: New Riders Publishing.

# EU data protection legislation and case-law with regard to biometric applications

**Ioannis Iglezakis**

## Introduction

The privacy implications of biometric applications employed in the private sector have been examined in the recent years by EU Member States' Data Protection Authorities (DPAs) in many occasions[1]. The progress in the development of biometric technologies and their application for authentication/verification or identification required the intervention of supervisory authorities, taken into account the privacy concerns raised by biometric technology, which could compromise informational privacy[2].

The decisions taken by DPAs, however, seem to be ambiguous and lack consistency. In particular, there is no consensus which criteria make biometric data processing lawful and there are different interpretations on the application of the proportionality principle to biometrics. The Data Protection Working Party established by Article 29 of Directive 95/46/EEC[3] delivered an opinion on biometrics on 1 August 2003 (WP 80, 2003), which did not had as an effect the harmonization of application of the EU data protection legislation to biometric systems (Liu, 2009, p. 327-238).

On the other hand, we are experiencing a proliferation of biometric systems in the public sector. Many states around the world, in order to combat identity fraud, included biometric data in passports, while other countries plan or have introduced biometric data (mainly fingerprints) in identity cards (Grijpink, 2006, p. 317). Currently, there is a burning debate about the implementation of biometrics in passports and ID cards due to problems of constitutional and data protection law, which are raised by it (Hornung, 2004; 2007).

These problems highlight the absence of clear rules on specific issues in the General Framework Data Protection Directive[4], but also the intricacy of the issues raised by modern technology with regard to data protection. Thus, the privacy issues raised must be addressed with adequate legislative and technical safeguards.

## Description of biometric applications

Biometric systems are applications of biometric technologies that consist in the automated measurement of behavioral or physiological characteristics of a human being to determine or authenticate their identity (Liu, 2009).[5] Such applications are employed for various tasks, in different areas and in the public as well as in the private sector.

Biometric features that are used for verification or identification have common characteristics. They are: a) universal, as they exist in all persons, b) unique, for they are distinctive to each person and c) permanent, since the property of the biometric feature remains permanent over time for every individual) (DPWP 2003, p. 3). Other properties of biometrics features are the following: a) collectibility: the biometric characteristic should be quantitatively measurable and easy to collect, b) performance: accuracy, speed and resource requirements should be satisfied, c) acceptability: indicates the extent to which a system is harmless and accepted by the intended users and d) circumvention: refers to the robustness of a system against fraudulent methods and attacks (Zorkadis and Donos, 2004, p. 127).

There are two main categories of biometric techniques, i.e. a) physical and physiological-based techniques which measure the physiological characteristics of a person and include fingerprint verification, finger image analysis, iris recognition, retina analysis, face recognition, outline of hand patterns, voice recognition, etc. and b) behavioral-based techniques, which measure the behavior of a person and include hand-written signature verification, keystroke analysis, gait analysis, etc. Yet, biometric systems exist that combine different biometric modalities of the use with other identification or authentication technologies.[6]

Apparently, biometric applications involve the use of unique biological and/or behavioral characteristics of a person, which are collected and stored for the verification of a claim, made by that person or for his/hers automated identification. The two basic functionalities of biometrics, which must be distinguished for the assessment of privacy risks, are: 1) the verification function, which is a one-to-one comparison, allowing an authentication check of a claim by a person, and 2) the identification function, which is a one-to-many comparison, allowing to verify that a biometric characteristic is in the central database or to identify to whom that biometric characteristic belongs (Kindt, 2007). Verification does not always require identification and also, it does not require that the biometric feature is stored in a central database, but it can be stored on a card in the possession of the user.

Biometric data can be processed after a biometric template is extracted from the biometric data (e.g. image of the fingerprint, picture of the iris, etc.). The biomet-

ric template, which is a structured reduction of a biometric image, is presented in digitalized form and is stored in a database. Alternatively, biometric processing takes place on the basis of raw biometric data (e.g. an image). The templates can be stored in the memory of a biometric device, in a central database or in plastic, optical or smart cards (DPWP 2003, p. 4).

Biometric data processing is used for the automated verification or identification purposes in order to provide secure access to physical (restricted areas, workplaces and other facilities) or virtual areas (to electronic systems or services) (DPWP 2003, p. 2). On one hand, it should be stressed out that biometric systems enhance privacy, as they are more secure and flexible than the traditional authentication procedures, e.g. those based on documents or codes that can be stolen, lost or forgotten. On the other hand, however, the processing of biometric data means enhanced control of the individual, compared with traditional authentication and identification procedures.

## The risks of biometric data processing

The privacy risks of biometric applications are emphasized by privacy activists, whereas data protection authorities also adopt a negative stance towards biometry (see below). At first hand, there is an association of biometry with criminality, since biometrics was initially applied in the area of DNA and fingerprint testing. Fingerprint testing has been used previously by law enforcement agencies for the investigation of crimes and their collection was subject to legal constraints. As a result, their use for verification or identification purposes provokes fears of increased surveillance over citizens or users of biometric applications and loss of dignity, as means of criminal investigation such as fingerprint testing are applied for identification and verification of common citizens (DPWP 2003, p. 1; Cavoukian, 1999).

In our view, the advantages provided by biometrics should not be ignored and, therefore, the assessment of privacy risks should consider the particular circumstances of biometric data processing. The main factors which must be taken into account are the purpose of the system, i.e. if it is used for identification or verification, whether biometric data are stored centrally or locally and whether a system allows the re-use of biometric data for incompatible purposes. Furthermore, a proportionality test should be applied, taking into account all the above criteria and the particular details of the processing.

Privacy concerns are awakened primarily when biometrics, e.g., fingerprints, are used for identification purposes and are stored centrally. In this way, biometric processing allows a person to be tracked individually and be subject to monitoring, since biometric features act as unique identifiers that bring together dis-

parate pieces of personal information about a data subject (Cavoukian, 1999). It is notable that nowadays the use of biometrics for identification takes place on a large scale in the public sector, since the adoption of EU Regulation No 2252/2004 imposing mandatory biometric features in passports and travel documents. In the EU, also several governments have introduced eID cards with biometric features and others are planning to introduce eID cards (Hornung, 2004).

Another reason for concern is the possibility offered by biometric applications that personal information from different sources be linked together to form detailed personal profiles about the individual. This infringes manifestly the right to informational privacy and therefore, measures should be taken to address this threat to privacy. Similarly, a risk to privacy emerges where the biometric data will be used for other purposes, i.e. for secondary purposes not compatible with the purposes for which the data were initially collected. This risk comes mainly forward when third parties have the ability to gain access to biometric data in identifiable form and bring them together with other information, without the consent of the data subject (Cavoukian, 1999).

The accuracy of data is an important factor for the assessment of biometric systems. In case biometric data are not accurate, this would lead to the false rejection of authorized persons and the false acceptance of unauthorized persons. Such instances jeopardize privacy, if a third person is identified in place of an authorized person or if the latter is being wrongly rejected (Kindt, 2007, p. 168).

Other privacy risks of biometric applications are also subject of research. Security threats may put at risk the functioning of biometric systems, such as the misappropriation of biometric data via spoofing. Additional information which is present in raw data may reveal sensitive information concerning health or revealing racial origin. It is thus suggested to destroy such unnecessary data (DPWP 2003, p. 7-8).

## The legal review of biometric applications by European organizations' opinions, Data Protection Authorities of EU Member States and national case law

An analysis of data protection problems of biometrics was delivered by the Data Protection Working Party (DPWP) in 2003 (op. cit), which identified some fundamental issues, stressing out the importance of the proportionality principle. The Consultative Committee of the 108 Convention (Consultative Committee 2005, p. 18) and the European Data Supervisor (EDPS, 2006, s. 2.4) also provided comments on the application of this principle in the biometric context.

The Working Party underlines that the purpose and proportionality principles must be observed. The purpose for which biometric data are collected and proc-

essed must be firstly determined. Furthermore, the principle of proportionality has to be respected. Article 6 of Directive 95/46/EC lays down, in more particular, that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. And also that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed (DPWP 2003, p. 6).

The Working Party also identifies other aspects that have to be addressed (DPWP 2003, p. 8). It refers to the principle of fair collection of information and to the legitimacy of processing, emphasizing that the processing of biometric data must be based on one of the grounds of legitimacy provided for in Article 7 of the Directive and in case sensitive data are being processed, the processing must be in conformity with the provisions of Article 8 of the Directive. The Working Party, further, suggests submitting biometric systems to prior checking by data protection authorities if systems are to be used that present specific dangers. It also highlights the obligation of the controller to take technical and organizational measures to protect personal data and particularly, to implement such measures from the beginning of the processing, especially during the phase of "enrollment", where biometric data are transformed into templates or images. Particular care should be taken in order to avoid false rejection of authorized persons and false acceptance of unauthorized persons, which could create problems on many different levels.

In accordance with the proportionality principle, which takes the most important place between the other legal principles that apply in the case of biometrics, it should be examined whether the purpose can be achieved in a less intrusive manner. With other words, if there are several appropriate measures that can be taken, the measure chosen must be the most privacy-friendly with regard to the purpose of processing.

The principle of proportionality is explained with reference to certain circumstances of biometric processing. The Working Party has the view that biometric systems related to physical characteristics that do not leave traces (e.g. shape of the hand but not fingerprints) create fewer risks for privacy. This applies also for systems related to physical characteristics which leave traces but do not rely on the storage of data in the control device or in a central data base. The Working Party in its opinion highlights that central storage or unnecessary storage for authentication should be avoided. It is not clear, however, from the opinion of the Working Party how should identification applications be assessed. As the central storage of biometric features is unavoidable for identification, one cannot totally exclude the implementation of biometric systems for this purpose, but a strict ap-

plication of the proportionality principle is considered necessary (DPWP 2003, p. 6 et seq.).

The Consultative Committee proposes the use of biometric templates instead of raw biometric images, which contain less sensitive information than the raw data. It is argued, however, that it is not realistic to avoid any possible link with sensitive data, as most biometric data unavoidably contain racial, health, physical characteristic information which could be sensitive data (Liu, 2009, p. 239).

The Working Party and the Consultative Committee add to those criteria the storage length of the necessary biometric data and stress that biometric data should not be stored longer than necessary (DPWP 2003, p. 8; Consultative Committee, p. 8). Finally, the European data protection supervisor underlines the sensitive nature of biometric data and calls for risk assessment before any biometric processing takes place. It evokes the requirements of the European Convention for the Protection of Human Rights and Fundamental Freedoms and its case law, which must be taken into account (European Data Protection Supervisor, 2006, p. 3).

In the legal review of biometric applications, DPAs of the EU Member States base their decisions on the proportionality principle, applying the aforementioned criteria. In more particular, they check whether biometric applications for identification and authorization purposes comply with the requirements of Article 6 of the EU Directive as transposed into their national law. However, the interpretation of the proportionality principle varies, even by the one and the same authority. For instance, the French CNIL refused to allow the use of fingerprints to admit children to a school restaurant, since it held that digital fingerprints would pose too many dangers for misuse and that it was excessive. However, it accepted the use of hand geometry for the same purpose in a school cafeteria, as it held that they would not leave traces and could not be misused for any other than the original purpose.[7] On the other hand, the UK DPA has accepted the use of fingerprints in similar circumstances, but it noted that certain precautions should be taken, such as the limitation of the purpose of processing, security measures and the destruction of data when it is no longer needed (Information Commissioner's Office, 2007).

The use of fingerprints at the workplace to control the presence of employees or verify compliance with working hours and, at the same time, prevent unauthorized conduct by employees, has been considered as infringing the proportionality by the Italian[8] and Greek[9] Data Protection Authorities, since it has been held that the purpose of processing can be attained by other, less privacy-intrusive systems, which do not impinge on privacy and do not involve an employee's body.

The Greek DPA has adopted a very restrictive approach to biometrics, which is in some extent contradictory. While it considered as lawful the processing of biometric data related to access control in security installations in the Athens Metro[10] and the Venizelos Airport[11], it did not allow a biometric system used to authenticate users to company sites and systems, as it held that the control of entry into the company's facilities could be achieved by less restrictive means, such as access cards without biometrics[12].

A general remark is that in the decisions of DPAs in the EU Member States the legality of processing plays a less significant role than proportionality. It is notable that the Greek DPA delivered a negative decision on the use of iris and fingerprint on a smart card for air passengers in the context of a European project on the verification of identity of air passengers, on a volunteer basis[13]. Although data subjects would participate in this experimental project with their consent, the DPA held that in accordance with the principle of proportionality, less intrusive measures could be used, such as the presentation of the passport together with the ticket and the boarding card. It is notable that a project for the identification of frequent travellers is operational at the Schirphol airport in the Netherlands, while in the UK the IRIS project offers to passengers who volunteer to undergo an iris scan in order to skip passport checks.

More recently, however, the Greek DPA changed its opinion and delivered an affirmative decision on the use of a biometric application in the airport of Macedonia, Greece.[14] It allowed the operation of an experimental project in the airport installations, in which users' authentication takes place with the encryption of fingerprints and the production of various biometric identities. The Authority took into account that biometric data are subject to pseudonymization in a way that the biometric identities could not reveal the original biometric data.

On the other hand, the use of biometric data in EU passports, which affects all citizens, was introduced as a mandatory requirement despite the privacy controversy relating to it. It should be noted that the EU Regulation No 2252/2004 was upheld by the ECJ in its decision of 18 December 2007.[15] The Court held that the measures provided for in this Regulation concerning the verification of the authenticity of passports are capable of guaranteeing and improving the effectiveness of checks on persons at external borders and therefore, it considered Regulation No 2252/2004 as a measure developing the provisions of the Schengen acquis.

Evidently, there is discrimination of biometric applications in the private sector as compared to applications in the public sector and thus, a discussion is necessary of possible legislative solutions.

## Legislative provisions on the processing of biometric data in EU Member States

The EU Directive 95/46/EEC has no specific provision on the processing of biometrics and thus, it has to comply with the provisions of the Directive, in general. Some statutes of EU Member States contain, however, specific provisions applying to processing of biometric data, which will be further scrutinized.

### *The Norwegian Personal Data Act*

The provision of Article 12 of Norwegian Personal Data Act 2000 states that:

> National identity numbers and other clear means of identification may only be used in the processing when there is an objective need for certain identification and the method is necessary to achieve such identification. The Data Inspectorate may require a controller to use such means of identification as are mentioned in the first paragraph to ensure that the personal data are of adequate quality.

This provision regulates the use of personal numbers and other means of identification such as fingerprints and other biometric data. It basically provides that "accurate identification means" such as biometrics are being used when it is necessary. The requirement of necessity is understood as an expression of the proportionality principle, since in accordance with the interpretations of this provision, the use of biometrics is not necessary when other less intrusive alternatives are available for achieving the reasonable security purpose (Liu, 2009, p. 242).

Therefore, this regulation is a specification of the proportionality principle and thus, its regulative value is that it enhances the visibility of this principle.

### *The Personal Data Protection Act of Slovenia*

The Personal Data Protection Act of Slovenia provides more detailed provisions on biometric data processing. In Article 6 Nr. 21 biometric characteristics are defined in the following way:

> Biometric characteristics-are such physical, physiological and behavioural characteristics which all individuals have but which are unique and permanent for each individual specifically and which can be used to identify an individual, in particular by the use of fingerprint, recording of papillary ridges of the finger, iris scan, retinal scan, recording of facial characteristics, recording of an ear, DNA scan and characteristic gait.

Such a provision can only indicate, of course, biometric features and could not be conclusive. Furthermore, the act includes a specific chapter on biometrics (Chap-

ter 3), which applies to processing in the public and private sector. The purpose of biometric processing is defined in article 78, which states that: "The properties of an individual shall be determined or compared through the processing of biometric characteristics so as to identify him or confirm his identity (hereinafter: biometric measures) under the conditions provided by this Act".

On processing of biometric data in the public sector, article 79 provides the following:

> 1) Biometric measures in the public sector may only be provided for by statute if it is necessarily required for the security of people or property or to protect secret data and business secrets, and this purpose cannot be achieved by milder means.
>
> 2) Irrespective of the previous paragraph, biometric measures may be provided by statute where they involve compliance with obligations arising from binding international treaties or for identification of individuals crossing state borders.

This provision specifies general principles of data protection, such as the principle of lawfulness, necessity and proportionality. In our opinion, it is untenable that the law states the particular reasons of identification and verification and it would sufficient to declare that processing should be carried out for legitimate reasons.

Regarding biometric application in the private sector Article 80 (1) states that:

> The private sector may implement biometric measures only if they are necessarily required for the performance of activities, for the security of people or property, or to protect secret data or business secrets. Biometric measures may only be used on employees if they were informed in writing thereof in advance.

This provision does not differ from the previous provision. It defines the purpose of processing more abstract and it allows the processing in the workplace, provided only that employees are informed thereof. Here again, it would be sufficient to state that the purpose of processing is necessary for the purpose of the legitimate interests pursued by the controller.

The provisions of paragraphs 2 – 5 introduce an obligation of prior checking of the processing (in case "the implementation of specific biometric measures in the private sector is not regulated by a statute"). The National Supervisory Body has to make a decision whether the introduction of biometrics complies with the act and the provision of paragraph 1. It also has to decide on the lawfulness of biometric systems controlling the presence at work of public employees.

### *Other laws*

Other laws of EU Member States regulate the processing of biometric data as sensitive data or provide for procedural rules, namely the notification of processing to the supervisory authority.

The Italian Personal Data Protection Code[16] provides in section 37 for the notification of the processing of biometric data to the Supervisory Authority.[17] Section 55, which applies in data processing by the police, imposes the requirements of prior communication to the Authority and measures and precautions aimed at safeguarding data subjects to be complied with.

The Data protection act of Luxembourg[18] provides in Article 14 that prior authorisation by the supervisory authority (national committee) must take place for biometric processing, which is necessary for the control of the identity of a person.

The Slovakian Act[19] provides for regulation of biometric data processing in the framework of the regulation of sensitive data (special categories of personal data). It defines biometric data as data of the natural person based on which the person is clearly and unequivocally identifiable, e.g. fingerprint, palm print, analysis of DNA, DNA profile (section 4 (1) lit. n). Furthermore, it provides that:

> Biometrical data may only be processed under conditions stipulated by a special Act, provided that: a) it expressly results for the controller from the Act; or b) the data subject gave a written consent to the processing.

The processing of biometric data is subjected to the rules on sensitive data, in two laws; namely, in the Czech Personal Data Protection Act of 4 April 2000 (Article 4 lit. b) and the Estonian Act of 1 January 2008 defines as sensitive data in § 4 (2).

## A possible legislative solution

The divergences in the application of the EU data protection legislation with regard to processing of biometric data and the uncertainty as regards the criteria and factors used to apply the proportionality principle lead to the conclusion that a specific provision should be introduced concerning the said processing. The regulation of biometrics should necessarily include firstly, a comprehensive definition of biometric characteristic, so that the field of application of the provision is clearly defined. Secondly, substantial rules must be introduced. In our opinion, the purpose and proportionality principles should be specified in the context of biometrics. The relevant provisions should include procedural rules, e.g. rules on prior checking etc., so that the supervisory authorities exercise control over biometric processing.

It should be noted that the purpose of the processing of biometric data is crucial and certainly it must be one that serves particular authentication/verification or identification needs. It is untenable to support the view that biometric application can only be accepted in special cases for access control to premises or facilities secrets file, as the Greek DPA stated in many decisions (see, e.g., No 245/9/20.3.2000 decision). The legality of the purpose has to be judged on the basis of the criteria for making data processing legitimate. Consent is an important criterion, but in order to satisfy the requirements of being freely given, specific and informed, data subjects must be fully aware of the risks entailed by biometric technology. Nevertheless, even if data subjects have consented to data processing, a proportionality test has to be applied.

The main difficulty with the application of the proportionality principle is that a case-by-case interpretation of this principle may lead into conflicting decisions of data protection authorities. Thus, to conclude whether a specific application is the most privacy friendly among others, certain circumstances have to be taken into account. Generally, superisory authorities take into account the type of biometrics, the method of collection, the type and length of storage and the security of the system. One cannot preclude certain types of biometrics and give preference to others. In particular, the use of fingerprints cannot be generally excluded and preference be given to hand geometry. A system using fingerprints can be allowed in certain circumstances, so for instance if security measures are taken and data are deleted when they are no longer needed.

Finally, already Article 20 of Directive 94/56/EEC oblige Member States to determine the processing operations which are likely to present specific risks to the rights and freedoms of data subjects and check that there operations are examined prior to the start thereof. It is evident that the processing of biometric data presents such risks and ought, therefore, to be subjected to prior checking. It is noteworthy that the DP Working Party suggests to submitting biometric systems to prior checking if they pose particular dangers, but it would not be clear for data controllers and data protection authorities when this is the case. Therefore, a general obligation to submit such processing to prior checking should be introduced.

It would be also advisable to submit biometric applications to privacy impact assessment. The same provisions that would provide for prior checking should provide that the controller must submit a privacy impact assessment, on the basis of which the supervisory authority could make a decision to allow or not the biometric processing under consideration.

## Endnotes

1. It is notable that biometric applications and genetic technologies have in common that the object of processing are unique physiological characteristics of the individual; hence, such processing allows an intensive control of the individual, in case anonymization techniques are not used.
2. In our modern information society, informational privacy is not conceived as the right to be let alone (Warren/Brandeis); it rather encompasses the claim for exercising control over one's own information (Westin, 1967).
3. OJ L 281 of 23/11/1995, p. 31.
4. For an assessment of the EU Directive see, e.g., Robinson et al., 2009. In this study, it is pointed out that the Directive serves as a reference model for good practice and harmonizes data protection principles, which permit flexibility, while being technology neutral, but is characterized by weaknesses, such as that the link between the concept of personal data and real privacy risks is unclear, etc.
5. Liu underlies that the term 'biometrics' is used to describe two different aspects of the technology, i.e. biometrics as characteristics, referring to measurable biological or behavioural aspects of the person that can be used for automated recognition and biometrics as process, referring to automated methods of recognizing an individual based on measurable biological and behavioural characteristics (Liu, 2009, p. 237).
6. So, to perform authentication, three different methods may be used jointly – based on something the individual knows (password, PIN), something he/she owns (token, smart card, etc.) and something he/she is (biometric feature). For instance one can be authenticated to use a computer by inserting a smart card, typing a password and presenting his/her fingerprint (DPWP 2003, p. 4).
7. CNIL, Deliberation 02-070 of 15.10.2002.
8. See The Garante per la protezione dei dati personali, Provision of July 21, 2005.
9. DPA, Decision of 20/3/2000.
10. DPA, Decision No. 9/2003, online available at: www.dpa.gr.
11. DPA, Decision No. 39/2004, online available at: www.dpa.gr.
12. DPA, Decision No. 74/2009, online available at: www.dpa.gr.
13. DPA, Decision No 52/2003, online available at: www.dpa.gr.
14. DPA, Decision No. 31/2010, online available at: www.dpa.gr.
15. Case C-137/05 United Kingdom of Great Britain and Northern Ireland v Council of the European Union. European Court reports 2007 Page I-11593.
16. Legislative Decreee no. 196 of 30 June 2003.
17. Garante per la protezione dei dati personali; www.garanteprivacy.it.
18. Texte coordonné de la loi du 2 août 2002 relative à la protection des personnes à l' égard du traitement des données à caractère personnel.
19. Act No. 428/2002 Coll. On Protection of Personal Data, as amended by the Act No. 602/2003 Coll., Act No. 576/2004 Coll. and the Act No. 90/2005 Coll.

## References

Article 29 Data Protection Working Party, Working Document on biometrics, 1 August 2003, (No. 12168/02/EN, WP 80), online available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf

Cavoukian, A. (1999). Privacy and biometrics, online available at: http://www.ipc.on.ca/images/Resources/pri-biom.pdf

European Data Supervisor (2006). Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organization of the reception and processing of visa applications (COM (2006 269 final) – 2006/0088 (COD) (2006/C 321/14).

Grijpink, J. (2006). An assessment model for the use of biometrics, Computer Law and Security Report 22, pp. 316-319.

Hornung, G. (2004). Biometric Identity Cards: Technical, Legal, and Policy Issues, in: S. Paulua, N. Pohlmann and H. Reimer (Eds.), Securing Electronic Business Processes, pp. 47-57.

Hornung, G. (2007). The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards, SCRIPT-ed, vol. 4:3, online available at: <http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/hornung.asp>

Information Commissioner's Office (2007). The use of biometrics in schools, online available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_final_view_v1.11.pdf

Kindt, E. (2007). Biometric applications and the data protection legislation, Datenschutz and Datensicherheit 31 (2007) 3, pp. 166-170.

Liu, Y. (2009). The principle of proportionality in biometrics: Case studies from Norway, Computer Law and Security Report 25, pp. 237-250.

Robinson, N., Graux, H., Botterman and M., Valeri, L. (2009). Review of the European Data Protection Directive, Technical Report, Rand Europe, online available at: http://www.rand.org/pubs/technical_reports/TR710/

The Consultative Committee established by the Council of Europe's Convention for the protection of individuals with regard to automatic processing of personal data of 1981 (2005). Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data, online available at: http://www.

coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf

Warren, S. & Brandeis, L. (1890). The right to privacy, Harvard Law Review (4), pp. 193-220.

Westin, A. (1967). Privacy and Freedom. Athenaum, New York.

Zorkadis, V. & Donos, P. (2004). On biometrics-based authentication and identification from a privacy-protection perspective. Deriving privacy-enhancing requirements, Information Management & Computer Security vol. 12 No. 1, pp. 125-137.

# Freedom of expression in cyberspace and the Coroner's and Justice Act 2009

**Maureen Johnson**

One half of the world cannot
understand the pleasures of the other.

Emma, Jane Austen

## The panic

The focus of this paper is pornography. More specifically anti-pornography law in the UK and more specifically still, law that prohibits pornographic images of children. For many people, this is a not a controversial area. Because they are convinced that the laws would never apply to them, they are happy that prohibitions are on the statute book to deal with the paedophiles in the community and beyond.

It may be however, that sometimes the law, particularly unquestioned and unchallenged, for whatever reason, can go too far and can become not only disreputable but counterproductive in its reasoning and its practicalities. The Coroners and Justice Act 2009 is a wide ranging piece of legislation which covers duties of coroners investigating deaths and in relation to treasure trove, as well as partial defences to murder, infanticide and assisting and encouraging suicide, genocide, conspiracy, evidence and treatment of witnesses. Amongst this rag bag of a statute, s62 to 69 cover the possession of a prohibited image of a child.

This act passed into law without media coverage except on the revised provocation criteria as a partial defence to murder. This is probably because much of the act is technical and procedural and would only invite comment from practitioners or the police, but s62 – 69 are of an altogether different order and will undoubtedly bring many unwise individuals within the remit of a personally disastrous offence.

## The Explosion

Before the 1970's, law enforcement authorities saw few indecent images of children, although it would be plainly untrue to say that sexual interest in minors did not exist before this time. Cultures throughout history have tolerated or encour-

aged the taking of adolescent boys and girls as sexual partners or brides. The age of consent for girls in the UK in the 1860s was twelve, raised to 13 in 1875 by Parliament. It wasn't until the late 19th century that the age of consent for girls was fixed at 16, where it remains today. As little as 130 years ago in the UK, many girls would have been married by the age of 16 and most of them would have been mothers. This is not to suggest that increased protection is a bad thing, simply that our concept and definition of childhood is plainly something that alters with time and cultural and religious heritage.

A British person in their late thirties can probably easily remember the British government of the day[1] outlawing the possession of indecent images[2] of children and members of the Paedophile Information Exchange – or PIE for short – demonstrating in the street at what they saw as a restriction of their liberty.

What is beyond doubt now however, is not just that there are more indecent images of children to be found, but they are probably much more extreme, involving toddlers, or even babies, and there is no doubt that people who produce or pay to view such images are – and should be – committing a serious criminal offence. These are the paedophiles of our nightmares. What has been surprising has been the number of people who have been 'caught looking' at indecent images of children. The famous 'Operation Ore' in the UK resulted in 7,000 suspects in the UK, of whom 3,500 were arrested and 1,230 convicted for possession of indecent photographs of children under s. 1 of the Protection of Children Act 1978. Among those convicted were teachers, doctors and members of the police force as well as previously convicted paedophiles. Several individuals committed suicide rather than face investigation and charge. These people, while undoubtedly still indulging in reprehensible criminal behaviour, are probably not what we imagine as paedophiles, and if asked to self-describe, would almost certainly not put themselves into that demographic. So what makes them look at such images, when the cost is likely to be so high? Privacy and imagined anonymity cannot be overlooked, but what should be a repressive force even in those circumstances might be a sense of guilt as to what was being seen and certainly funded by an individual's decision to view such material. A person' feelings of guilt can undoubtedly be lessened by the remoteness he feels from the situation and the perceived permissiveness of the internet culture. Giddens[3] describes guilt as carrying

'the connotation of moral transgression: it is anxiety deriving from a failure, or an inability, to satisfy certain forms of moral imperative in the course of a person's conduct.'[4]

He goes on to suggest that the diminution of guilt in modern society is as a result of the erosion of Society itself in late modernity and because of this, the experience of self becomes increasingly inwardly reflexive as the moral community

which previously held it in check diminishes or fragments. If this is true of the society in which we live with its permissiveness and wider tolerance of sexual difference, it is probably fair to say that the theory is even more relevant to the online society in which many viewings or exchanges of indecent material take place. This is a new society which is feeling its way, and encourages free and frank exchange of views and makes a speciality of embracing the abnormal and disenfranchised. It is, in short, a perfect place to be accepted, and a perfect place to hide. People simply do not link their behaviour on line as transgressive, because they feel free from the pressure to conform. Much has been made of the importance of the internet as a place of escape into fantasy worlds where the impossible becomes real, and an individual can be rid of their reality, where a person can fly, or be tall, or be a member of the opposite sex. There may be more discomfort about the internet as a place where a person feels that the person they actually are can escape from the unreal persona they have to present to the real world, which would reject them if it knew of their true face. There is something to be said of the internet as a place of masks and deception. It must be realised that just as many people are taking their masks off online as are putting them on.

And some of them are people whose reality society does not approve of.

It needs to be clear that I do not for one moment think that laws protecting our children are too tough, but it also has to be accepted that there is a section of society for whom the sexual interest in younger people is a fact of their lives. Ignoring this section of society will not make children safer, nor will it make them go away. Criminalising anything that looks as though it might be attractive to one of these people is spreading the net too wide and risks sweeping many into the laws grasp that should not be there, with terrible consequences for their lives. The Coroner's and Justice Act 2009 has made it illegal to sketch a picture of a naked child which is drawn by the defendant and shown to no one else. If that still sounds a reasonable law to have, the definition of a child - discussed later in this work - may give pause for further thought.

## The legislation

The protection of children from exploitation and damage within the pornography industry has rightly come a long way in the last 22 years, before which it was legal[5] in the UK to possess indecent photographs of children as long as a person didn't produce them and had no intention of showing or distributing them[6]. From here the law has moved to keep pace with photoshop technology by making criminal the possession of pseudo-photographs[7] - defined by Lloyd as

"what appears to be an indecent image of a child, which is made up of a collage of images, modified by the use of computer painting packages, none of the elements of which is indecent in itself."[8]

The inclusion of pseudo-photographs could be seen as controversial in two ways. One was the inclusion of the word 'make' within section 1 of the PCA, where previously it was a prohibited act to 'take' an indecent image of a child. Although the word 'make' was intended to refer to the pseudo-photograph, it quickly became established that a person downloading an image from the internet could be convicted of 'making' a photograph, with the implied nexus to the abuse shown. This meant that a possession offence under s160 CJA 1988 carrying a maximum of five years imprisonment could be charged as a s1 PCA offence carrying a ten year maximum sentence if a person obtained the image from a computer system. This may be justified as the market for such images would be diminished if consumers did not keep up the demand for them, but it creates a dichotomy between an online and offline offence which is far from ideal.

The second controversy rests on the notion of harm. A realistic image which is created without harm to an individual is therefore prohibited by the inclusion of pseudo-photographs in the PCA 1978 and to a certain extent the role of fantasy in an individual's private sphere of his/her sexual life has already been curtailed significantly. In the American case of Campbell, a man had superimposed young girl's heads onto the bodies of adult women to 'see what they would look like when they were older'. It was accepted by the prosecution that the man had not contacted the girls in any way, and one of them appeared to be the 'Hannah Montana' character from American television and film. The actress who plays Hannah Montana, Miley Cyrus, was nearly 17 years old at the time of the charge. The Assistant District Attorney[9] is quoted as saying,

"When you have the face of a small child affixed to the body of a mature woman, it's going to be the State's position that this is for sexual gratification and that this is simulated sexual activity."[10]

According to UK law, an indecent pseudo-photograph will be illegal if it 'appears to be a photograph'[11] and shall be treated as a child if 'the predominant impression conveyed is that the person shown is a child, notwithstanding that some of the characteristics shown are those of an adult.'[12] An image therefore has to pass a test of some objective realism before there could be a conviction.

Even since this stage legislation in the UK has progressed rapidly, to keep up with the alleged depravity in the digital environment. In 2008 the unloved s69 (3) of the Criminal Justice and Immigration Act made it an offence to possess an illegal image which had been 'derived from' a photograph, which presumably cov-

ers morphed Computer Generated Images (CGI's) and freehand drawings 'copied' from a photograph or pseudo-photograph, but does not cover a product of the artists imagination. With the disquiet about the effectiveness of s 69(3)[13] Parliament moved quickly to 'plug the gap' left for internet predators by bringing in s62 of the Coroners and Justice Act 2009 which makes it illegal to be in possession of non-photographic 'prohibited images of a child ..... produced by any means.' A prohibited image is one that is:

(a) pornographic[14]

(b) falls within subsection 6, and is

(c) grossly offensive, disgusting or otherwise of an obscene character.

At first sight s62 is an admirable piece of legislation. It closely mirrors s63 of the CJIA 2008 which prohibits 'extreme pornography'[15], the language of the section is straightforward in addressing what many might consider a social evil of epidemic proportions and it requires the specific consent of the DPP for a prosecution to be brought. However, s63 of the CJIA 2008 contains an important codicil in that ;

'a reasonable person looking at the image would think that any such person or animal was real.'[16]

S62 carries no such limitation and therefore there is apparently no legal demand for objective realism of the prohibited image. This takes the law into entirely new territory. While there may have been an argument that pseudo-photographs and genuine photographs were too alike to tell apart, with the extra burden it may have put on the prosecution to prove actual abuse, that argument cannot be made under s62 which clearly prohibits work of the artist's imagination in any medium[17].

Those who have to obey the law are then faced with a crime they may not have anticipated and - thanks to the upset that the mention of child pornography often engenders - know little about. For reasons that may be obvious, and may be legitimate, when a person accused of being in possession of illegal images of children is arrested or charged, the public usually know only the number of such images in the defendant's possession. Left to imagine, we imagine the worst, a young girl or boy somewhere raped or tortured for sexual kicks, perhaps repeatedly, and righteous condemnation follows. The truth in any given case may be more prosaic, may be something many of us have seen or rolled our eyes at, and may arguably even be a breach of an individual's freedom of expression or his right to privacy under Art. 10 or 8 respectively of the Human Rights Act 1998[18]. This paper will be asking, objectively, and hopefully away from the heat of hysteria, if s62 of the Coroners and Justice Act has gone too far in proscribing the rights of an individu-

al to admit to his own private sexual fantasies, with no corresponding consolidation of the rights of another who should be protected.[19]

In the case of *R v Kingston*[20] Lord Taylor CJ in the Court of Appeal said

"Having paedophilic inclinations and desires is not proscribed; putting them into practise is."

It would seem that in the face of this legislation, his first assertion is now untrue under English law. However, as s62 CJA did not come into force in the UK until 10th of April 2010 there have understandably been no prosecutions as yet under it. It might be helpful to look to other jurisdictions and the similar phraseology under s63 CJIA 2008 in order to ascertain how our own legislation may be applied. Consider the following case law.

### *McEwen v Simmons*[21]

This is a fairly recent Australian case concerning an appeal by McEwen against his conviction for possession of child pornography. S 91H(3) of the Crimes Act 1900 (NSW) reads;

'child pornography.....material that depicts or describes, in a manner that would in all the circumstances cause offence to all reasonable persons, a person under (or apparently under) the age of 16 years (a) engaged in sexual activity, or (b) in a sexual context....'

McEwen was in possession of spoof 'Simpsons' cartoons where the 'ten year old Bart' and 'eight year old Lisa' were portrayed as being engaged in sexual acts.[22]

This was followed by the case of Milner[23] who was convicted on the strength of Simpsons and Powerpuff Girls cartoons which the police managed to retrieve from his computer's recycle bin a year after the machine was seized. He claimed to have downloaded the images to show them to a friend because he 'thought they were funny'.[24] He was jailed for 12 months, suspended for five years, fined $1000 and has to sign the sex offenders register. Ironically, in 2003 he received just two years probation for being found with 59 indecent images of real children on his computer.

### *US v Whorley*[25]

Whorley appealed against his conviction for possessing Japanese Anime cartoons which contained depictions of children engaged in sexual acts, and for sending and receiving emails containing discussions of children being involved in sexual activity. The appeal was dismissed, but there was dissenting judgment, based on the minimal – or non- existent – harm that the fantasies involved.

### *R v Holland*[26]

Holland was charged initially with two offences under the CJIA 2008 possession of 'extreme pornography'. One charge related to a film clip featuring bestiality, and the other to a short clip containing two women. The first charge was dropped after the 'animal' involved was revealed to be a spoof of a cartoon tiger from a breakfast cereal advert, but Holland pleaded guilty to possession of the other, saying he had been sent it as a joke but had forgotten to delete it. The clip apparently involved two women, coprophilia and vomit[27]. He was warned to expect a custodial sentence.

## The Rights?

These cases come from different jurisdictions with differing legal jurisprudence, trying essentially to grasp the same nettle. How far should the law intrude into a person's private expression of his or her sexuality where there is no harm or risk of harm to another, and has a person a defence that he should be left alone in certain areas of his life?

## Constitutional Rights

Jurisdictions with a written constitution to uphold the rights of the citizen against the state seem to fare better in this respect. The case of *R v Sharpe*[28] before the Supreme Court of Canada held that a virtual or created image of a non-real child could not be prohibited by legislation when kept for the private purposes of the creator:

'This definition of 'child pornography' catches depictions of imaginary human beings privately created and kept by the creator. Thus, the prohibition extends to visual expressions of thought and imagination, even in the exceedingly private realm of solitary creation and enjoyment…'

Similarly in the United States of America, sections of the Child Pornography Prevention Act 1996 were challenged as unconstitutional under the First Amendment as they prohibited (inter alia)

'visual depiction is *or appears to be,* of a minor engaging in sexually explicit conduct' (emphasis added).

In Ashcroft, *Attorney General, et al v Free Speech Coalition et al*[29] the Supreme Court Justice commented that there had been a failure to show a causal link between CGI images and harm to real children, he also stated in the judgment;

'First Amendment freedoms are most in danger when the government seeks to control thought or justify its laws for that impermissible end. The right to think is the beginning of freedom, and speech must be protected because it is the beginning of thought.'

## ECHR Rights

In Europe the legislation most often used in an attempt to protect a perceived breach of an individual's rights to freedom of expression and to his privacy are Articles 10 and 8 respectively of the European Convention of Human Rights, enacted into UK law as the Human Rights Act 1998. Most people are familiar with Art 10(1);

'Everyone has the right of freedom of expression. This right shall include freedom to hold opinions and to receive and impart information without interference by public authority....'

Qualified by Art 10(2);

'The exercise of these freedoms, since it carries with it duties and responsibilities may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety for the prevention of disorder or crime, for the protection of health or morals for the protection of the reputation or rights of others....'

As 'expression' has been held not to apply to just speech but to many forms of self-expression[30] a complaint of a breach of this right has been a classic defence to pornography possession or production. It has also been held to encompass the right of a person to receive information, not just to express it. The European Court of Human Rights has held that freedom of expression is:

'Necessary for individual self fulfilment and an essential foundation of a democratic society. A democratic society, characterised by pluralism, tolerance, and broadmindedness, is a necessary condition in which human rights can be protected and justice and peace can flourish.'[31]

In return, the protection of morals is cited as a justification for a prosecution, and States have traditionally been allowed a wide margin of appreciation by the European Court of Human Rights and been held to have acted within their discretion viz-a -viz the protection of morals[32] under their jurisdiction. However, in the case of *Muller*[33] the court found that this margin was not at odds with an individual's right to express himself in a way that may 'shock, disturb and offend the state or any section of the population'.[34]

In order for the protection of morals to prohibit the freedom of a person's expression, the prohibition must be proscribed by law and be necessary in a democratic society. With the advent of s62 of the CJA 2009 the drawing of a naked child can be said to be proscribed by law, but is such a prohibition necessary? The necessity of a prohibition will rest upon whether or not it is a proportionate way of meeting a pressing social need. There is – of course – a pressing social need to protect living children from abuse, but whether s62 is a way of meeting that need could be debated. It is worth remembering again that there are no children involved in the making of the material in question and the CJA recognises the distinction between harm to real children and this new offence by restricting the maximum sentence for s69 to three years as against 10 years for a PCA offence. In a recent Home Office consultation paper it is stated:

'We are not aware of any specific research carried out to ascertain whether there is a direct link between possession of these (cartoon) images and increased risk of sexual offending against children.'[35]

It has been argued extensively that images such as these can be used to lure children into abuse by presenting a normalised view of sexualised behaviour and therefore the legislation is necessary to prevent an indirect 'harm' to these children. The Sexual Offences Act 2003 covers specific scenarios, such as S10,[36] A person found showing pornographic pictures to a minor could arguably be charged with this offence, or s12,[37] which covers 'looking at an image of any person engaged in ...sexual activity.[38] The maximum term of imprisonment for the incitement offence is 14 years, so the potential problem of an individual using non-photographic images to normalise aberrant sexual behaviour appears already to be taken account of in criminal statute, further bringing into question the 'necessity' of s62 as a protective measure for children in society, as well as the proportionality of the measure of the restriction to the rights of individuals as against the harm prevented. The illegality of non-photographic images of children, if deemed to be in the prohibited category, is subject only to the defences of 'legitimate reason for possession', 'did not know or have cause to know it was a prohibited image of a child' or 'was sent the image without prior request and did not keep it for an unreasonable period of time.'[39] These defences closely mirror the PCA 1978 defences, and raise the issue of the meaning of 'legitimate reason for possession', which has not been defined in either act. The CPS on its website states that the defences cover those who have a 'legitimate work reason for being in possession of the images'.[40] This might cover doctors or the police or a barrister preparing a case. The courts seem to have been dismissive of individuals claiming academic research as a legitimate reason, possibly with good reason, but this defence is based on the reverse burden of proof where it is for the defendant to prove he had a legitimate reason for the possession. It seems unlikely

that a person who has produced non-photographic images for their own private use, or has a downloaded cartoon or Anime in their possession would be able to prove legitimate use to a juries objective satisfaction under s64.

It would seem that a person pleading a breach of his Art 10 rights because of a charge under s62 has little chance of success. Pornography *per se* has traditionally been viewed by the judiciary within the UK has having few redeeming features worthy of protection under Art 10 that are not trumped by the margin of appreciation allowed to states under the protection of morals. However, cases such as *Handyside* and *Muller* were decided partially upon the rights of others not to be unwittingly exposed to expression they might find disgusting and the protection of children from the material that was freely and publicly available. If those rights are not engaged, perhaps because an offence under s62 prohibits the mere possession of privately created and held material which causes (certainly) no individual or (arguably) societal harm, then the protective mechanism of the law must be focussed upon the creator and possessor of the item himself. This is nothing new in English law. *In DPP v Whyte*[41] the Court of Appeal held that the Obscene Publications Act 1959 is not intended to focus on the harm that might be inflicted on another but is intended to protect the minds of those who are likely to encounter the obscene work in question:

'Influence on the mind is not merely within the law, but is its primary target.'

It must be questioned how far a democratic society should go in an attempt to impose a paternalistic norm on a minority interest within it and how a denial of an expression of self - which a person's sexuality undoubtedly is – will affect that individual's notion of selfhood.

Given that the expression of a sexual identity is part of the concept of an intimate self-knowledge, perhaps the prohibition of non-photographic images is better approached under Article 8 ECHR;

'Everyone has the right to respect for his private and family life, his home and his correspondence.'

Subject to article 8(2):

'There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

In the case of *Bruggerman*[42] the Court of HR said

(Art. 8) 'also secures to the individual a sphere in which he or she can freely pursue the development and fulfilment of his or her personality.'

Here again, the UK courts have been undecided on the relevant sphere in which an individual can flourish unmolested and their conclusions have been far from consistent. In the famous case concerning sado-masochistic homosexuals[43] it was held that consent to the bodily harm suffered by one of the individuals was not a defence to a charge under s47 of the Offences Against the Person Act 1861 as such a defence:

'for the purpose of satisfying a sado-masochistic libido were not in the public interest.'

This contrasts with the case of *Wilson*[44] where the court decided that there were no public policy or public interest reasons why the appellant's branding of his wife's buttocks with a hot knife – apparently at her insistence – should be subject to criminal law.

These cases were decided before the Human Rights Act 1998 came into force and were heard in UK courts, but the case of *Dudgeon*[45] may be of relevance here.

Mr Dudgeon complained that a statute prohibiting private homosexual acts between consenting adults breached his rights to privacy under the Art 8 of the European Convention. The Court held at para 41:

'The maintenance in force of the impugned legislation constitutes a continuing interference with the applicant's right to respect for his private life (which includes his sexual life) within the meaning of Article 8(1). In the personal circumstances of the applicant, the very existence of this legislation continuously and directly affects his private life either he respects the law and refrains from engaging.... In prohibited sexual acts to which he is disposed by reason of his homosexual tendencies, or he commits such acts and thereby becomes liable to criminal prosecution.'

Clearly there are differences here between consenting adults and an act involving a child who cannot consent, and the Court was careful to point out that legislation may be necessary to protect the vulnerable, particularly the young. In our discussion, there are no acts, there are no children, but the legislation, as has been seen, will directly and continuously affect an individual's sexual life, with a choice either to forebear or to face prosecution. There will be those who argue that the law should enforce forbearance in such a circumstance, and that the paternalistic norm should prevail, but part of the concept of a democratic society is the care and tolerance it displays towards minority interests. In arguing that we have become less tolerant as a society, Alan Norrie[46] suggests that the outcome of the twentieth century's drift into equality legislation has the effect of making society less equal as we display alarm and anger at those who are not capable of

being brought 'into the fold' of normality, whatever that is. Equality legislation insists upon us all being equal and there is little room for transgressors.

Morals are concerned with the principles of right and wrong behaviour and with the goodness or badness of human character. This can be seen as conforming not to the physical or practical elements of humanity, but rather to the psychological aspects of a person's life – his thoughts and feelings, indeed the very characteristics that make that person who he is. There may be a valid argument of seeking to prevent harm to actual children by allowing animated or artistic images as a necessary means for an individual to express his or her private sexuality.

## The Coroners and Justice Act 2009

### *Is it a 'child'?*

The Coroners and Justice Act accepts that one of the points of the legislation is that a reference to an image of a child includes reference to an image of an imaginary child[47]. This seems a straightforward concept, but may be open to a much wider interpretation than intended. Is imaginary the same as fictional for instance? The *Whorley* and *McEwen* cases rest on what was referred to in the judgment as a 'representation' of a person – an image that was understood, while not being an actual person, as being person-like. In his comments on the *McEwen* case, Adams J was troubled by defining a character in a cartoon such as this as a person, even an imaginary one. He wondered how 'realistic' such a character had to be to make it a visual representation of a person, and whether the cartoon of an animal with some human characteristics would still amount to such a representation. Would Mickey Mouse have sufficient human characteristics to be the representation of a person, or Donald Duck?

Is imaginary the same as virtual? There has been debate about the freedom of individuals on line in virtual games such as Second Life, to 'age play' so that their characters assume the physical dimensions of children who can then form 'sexual relationships' with 'adult' avatars, in spite of all the players involved being over eighteen years old in real life. Is a small avatar to be taken as a 'child'? According to legislation, if it is an imaginary child, it would appear so.

## Image versus text

A dichotomy in the prohibition of materials which sexualise under eighteens is the law's horror of the image, as opposed to its relatively relaxed outlook on textual description of child/adult relationships. In *Whorley* the dissenting judge Gregory J said

The content of the emails can be described as 'a series of engaging in fantasies on the internet... The economic and social justification for regulating email fantasies

– even those involving activities that would be criminal if those fantasies were acted out – are minimal. Indeed, the harm, if any, involved in Whorley's conduct is not readily discernible because the emails were written and exchanged for the sole 'enjoyment' of Whorley and his counterpart... real children were not harmed, (or even discussed) during the 'production' of these emails.

The judge went on to mention authors, books[48] and films which have focussed on adult/child relationships, and to use them as examples of such works having 'redeeming social value' which the Government should not suppress as it would not aid in 'protecting the victims of child pornography' or 'the destruction of the market for the exploitative use if children.'

In the UK the dichotomy between how the law views the image and the written word is as acute. Unless text is capable of being brought within the remit of the Obscene Publications Act 1959[49], there appears to be no prohibition on text based descriptions of indecency with or between children, it is only the image that is forbidden. This might raise questions about the kind of behaviour the CJA 2009 is trying to prevent. If a 'virtual child' on Second Life – which are not overly realistic – is capable of being a paedophilic image, and being used to encourage offending, why isn't a sexually explicit story treated in the same way? It would be easy to argue that a written description of an event or series of events has more power to shock or delight than a pictorial representation. The picture is factual and limited to its parameters, but the text is constrained only by the individual's imagination. This further undermines the rational for the prohibition of non-photographic images.

## Image v. Reality

Perhaps the biggest nonsense concerning the current crop of 'anti-paedophile' legislation is that in the UK it is legal to have a physical relationship with a child from the age of sixteen for both males and females, but it is not legal to look at a pornographic picture of either of those classes of person until they are eighteen[50]. There are defences available under s1A of the PCA 1978, based on marriage, a civil partnership or 'living together as partners in an enduring family relationship' - although how enduring this has to be is unclear. These defences are not included in the CJA 2009, so while an indecent photographic image of a 17 year old bride or groom is no offence if consensual and private, a pencil sketch would be a breach of s62, unless the defendant can prove a 'legitimate reason' for possession.

## Images v. Prevention

Images of child abuse are sadly, always going to exist and there will always be demand for them. The fight against wicked acts being perpetrated on children should continue apace, as should the fight against those that fuel the industry by

buying photographs and films of the abuse. In the *Milner* case, the judge handed down a harsher sentence on the basis that Mr Milner had already been convicted for possession of indecent pictures of (real) children. It may be seen as telling that no further images of (real) abuse were found on the defendant's computer, only cartoon ones. A perfect example, surely, of someone who has been chastised by the law and changed his behaviour in a way that is beneficial to both himself and society – the criminal law acting as it should.

The UK's policy on indecent images may have gone too far. They purport to protect from an indirect harm that is unproven and probably unprovable and in doing so they restrict the freedom of citizens and may increase the risk of harm to living children. In the Consultation Paper on the Possession of Non-photographic Visual Depictions of Child Sexual Abuse[51] the Home Office stated:

'We are aware of a case where the police were unable to prosecute because the suspect was only found in possession of drawings and cartoons: no illegal photographs or pseudo-photographs were discovered.'[52]

No illegal photographs of an abused child in a suspect's possession should be a cause for relief, not disappointment that a charge is unable to proceed. In this situation at that time, the suspect had chosen not to break the law, he had not purchased or accessed images of child abuse and therefore not contributed to the market for such images with their resultant harm. Such a person now has that choice removed from them and a charge under s62 CJA 2009 would be able to be brought and would probably succeed. This would seem to reduce the incentive for a person not to go for the 'real thing' if he risks a criminal conviction in either event. Without an unprecedented and frankly unimaginable global crackdown and international cooperation, abusive images of children are going to be available on line. The CJA does not help these children, it does not work against the sites – usually based abroad – that perpetrate them, and there is no proof that the images it prohibits cause direct or indirect harm to any child at all. Morally, we may not like an individual's private fantasy world, and the world wide web enables those fantasies to be closer and more coloured that ever, but the law should pause before it makes criminal a person's private sexual landscape whether expressed through fantasy text or fantasy image. This is particularly so when there is a dichotomy between the application to the internet via emails and downloads and through hard copy books and pictures and the former hold evidential context long after the latter could be destroyed.

These cases discussed today show that images widely available on the internet and often passed between friends, particularly young men as 'a bit of a laugh' are now capable of giving those individuals a criminal record for possession of child pornography. Any criminal conviction can seriously hamper a person's future and life chances, but it must be obvious that an offence of this type will be viewed by the majority of

the public as one which signals the defendant has been involved in the actual abuse of living children, with the revulsion and outrage that such an offence will engender. In some cases brought under the CJA 2009 that couldn't be further from the truth.

## Endnotes

1. The Conservative government under Margaret Thatcher.
2. Criminal Justice Act 1988 s 160.
3. Giddens, A (1991) Modernity and Self Identity, Oxford: Polity.
4. *Ibid* p 153.
5. S1(1) Protection of Children Act 1979 – It is an offence to take or permit to be taken any indecent photograph of a child or to distribute or show such a photograph or to have it in possession with an intention to distribute or show it.
6. S160 Criminal Justice Act 1988 amended s1(1) of the Protection of Children Act 1979.
7. S84 Criminal Justice and Public Order Act 1994.
8. Lloyd, I., Information Technology Law Oxford University Press, 5th Edition (2008), page 254.
9. Dave Denny (Chattanooga, Tennessee).
10. CNN.com.
11. S7(7) PCA 1978.
12. S7(8) PCA 1978.
13. See 'Camera Obscura – the CJIA 2008 and Virtual Pornography'.
14. Definition of pornographic is based on a 'reasonable assumption' and is therefore objective.
15. 'It is an offence for a person to be in possession of an extreme pornographic image'.
16. S63(7) Criminal Justice and Immigration Act 2008.
17. See comments over the display of the 'Warren Cup' at the British Museum.
18. 'Everyone has the right of freedom of expression. This right shall include the freedom to hold opinion and to receive and impart information without interference by public authority……..'.
19. For a criticism of 'neutral academic discussion on pornography' which 'lacks emotion and humanity' see The Reality of Pornography – Clare Phillipson – McGlynn, C., Rackley, E., and Westmarland, N.(eds)(2007) Positions on the Politics of Porn. A debate on the government plans to criminalise the possession of extreme pornography, Durham: Durham University.
20. (1994) 3 All ER 353 HL.
21. (2008) NSWSC 1292.
22. Brian Simpson - *Controlliang fantasy in cyberspace: cartoons, imagination and child pornography* ICTL Vol 18 Issue 3.
23. http://www.qt.com.au/story/2010/01/26/an-ipswich-man-has-admitted-downloading-graphic-ca/.
24. Ibid.
25. United States Court of Appeals, 4th Circuit, December 18, 2008.

26. Unreported – Mold Crown Court – see PoliceSpecials.com –' Man could face prison over six second porn clip' 13th April 2010'.
27. It isn't entirely clear how this is 'extreme pornography' as opposed to pornography. In order to be extreme, it must conform to s7 – must be life threatening, or likely to result in serious injury, or involve a human corpse or an animal – none of which are apparently present here.
28. (2004) B.C.J. No 1565; 2004 BCSC 240; 2004 BC.C. LEXIS 1676, Judgment: February 20, 2004.
29. 535 U.S. 234 (US Supreme Court 2002).
30. For instance music, dancing or choice of clothing.
31. *Handyside v United Kingdom* (1979 – 1980) 1EHRR 737 (para 49).
32. See for instance *R v Perrin* [2002] EWCA Crim 747.
33. *Muller v Switzerland* (1988) 13 EHRR 212.
34. Although in this case the circumstances of the exhibition made the offences within the state's margin of appreciation.
35. Home office consultation paper on the possession of non-photographic depictions of child sexual abuse p6.
36. Causing or inciting a child to engage in sexual activity.
37. Causing a child to watch a sexual act.
38. S12(1)a SOA 2003.
39. S64 (1) CJA 2009.
40. https://www.cps.gov.uk/legal/p_to_r/prohibited_images_of_children/#a15.
41. (1972) AC 849.
42. Bruggerman and Scheuten v Germany [1977] D + R 10 para 55.
43. Brown [1993] 2 All ER 75, [2003] Crim LR 583.
44. (1996) Crim LR 573, CA.
45. *Dudgeon v United Kingdom* ECHR 23rd September 1981.
46. Law and the Beautiful Soul – Glasshouse Press.
47. *De Reuck v Director of Public Prosecutions and Others* (2004) 4 LRC 72 (South African Constitutional Court).
48. For example Lolita, The Color Purple and Absolom, Absolom.
49. S1 – an article is obscene if it 'tends to deprave and corrupt persons who are likely to see it.'
50. Sexual Offences Act 2003 s45.
51. Available at http;//www.justice.go.uk/publications/non-photographic-depictions.htm (30th June 2008). The consultation period ran from 2nd April 2007 to 22nd June 2007.
52. Ibid. Page 4.

# Examination of the relationship in the creation of advertising messages and issues of intellectual property in the digital era

**Androniki Kavoura &**
**Evgenia Bitsani**

## Introduction

Advertising may be considered as an entreprenual activity where many parties are involved such as businesemen, agents, media but may be also considered to be part of modern art [Zotos, 2008: 33; Thlikidou-Stogianni, 2003: 87].

Issues which are examined with the highest frequency according to legislation and advertising mainly focus on advertising and medical products, where it has been found for example, that in USA, justifications are made in advertisements aiming at minorities for food substitutes which should be prohibited [Chung, Hwang and Kim, 2007] or for advertisements aiming at children [Cross 2002 cf Gao, 2005] following a different way of dealing with advertising than in Europe.

On the other hand, references to issues of ethics, of influence that non acceptable types of advertising or of insulting advertising may have to people [Balasubramanian, Karrh and Patwardhan 2006; Russell and Belch 2005; Russell and Stern 2006] or the understanding of the way consumers see advertising which is not following the legal elements and may cause reactions [Gulas and McKeage, 2000 cf Drumwright and Murphy, 2004: 8], are very few.

Some argue that advertising is different from most other copyrighted work because an increase in advertising created as a result of copyright protection may not be beneficial to and desired by the public [Ramsey, 2006: 191]. Greece and other countries in Europe do not explicitly consider intellectual property right for advertising as is the case in USA. In regard to intellectual property, there is a defence of intellectual property rights that takes place in Bottis and Spinello [2009] and there is also the valuable work of the International Encyclopaedia of Laws which incorporates legislation from countries in the world and Greece is also included with the characteristics of Greek legislation [Bottis, 2003]. An issue, then, is raised regarding advertising, or better its content, and whether or not is included in legislation regarding protection of intellectual property and cultural resources.

The paper aims to present the way the US copyright law protects advertising, considering it to be intellectual property where legislation stands for advertising as well as for e-commerce and websites, providing information on types of intellectual property rights. Reference is then made to European legislation regarding advertising focusing on Greece as part of the European Union where European directives are implemented. Then, advertising's connection with intellectual rights is argued.

In 1903, the Supreme Court in USA concluded -for the first time- that advertising was within the protection of U.S. copyright law because of the difficulty of distinguishing between commercial and fine art [Bleistein v. Donaldson Lithographing Co., 188 U.S. 239, 251–52 (1903) cf Ramsey, 2006:191]. Nowadays, it is referred to as "commercial" art-to the protection of copyright statutes. Congress has already determined it is possible for courts to distinguish between advertising and other works because it excluded "advertising" from protection under the Visual Artists Rights Act, a 1990 amendment to the U.S. Copyright Act 17 U.S.C. § 106A; 17 U.S.C. § 101 [definition of a "work of visual art" protected under 17 U.S.C. § 106A excludes "advertising" cf Ramsey, 2006: 193].

Implications may exist from the adoption of such a system for advertising from one country to the other and caution needs to be taken [Bottis, 2004a]. The person in charge of advertising communication, should be aware of these issues contributing in that way, to the best presentation of advertising messages within a legal framework in the information age that advertising takes place.

## Advertising as a subject of protection of intellectual property

The object of the right of intellectual property is consisted of all the intellectual creations of their creators, which is intellectual work, as are the intagible resources [Bitsani, 2004] while cultural resources is the result of human activity which provide information for all sectors (socio economic or political) [Bitsani, 2004: 4].

These cultural resources are connected to their creator and this relation is sealed by the right of intellectual property which incorporates rules, protecting creators of work of speech, work of art and science, as is mentioned for example in Greek Law 2121/1993 entitled "Intellectual Property, related rights and cultural issues" which was amended by Greek Law 3057/2002 regarding intellectual property and cultural issues. Although there is no reference there in advertising per se but only in audiovisual works of the creator, allowing someone to initially exclude the content of advertising messages from these works -since it is not written in these words in legislation per se,- it is stated that every intellectual work of speech, work of art and science which is original, is protected from the right of

intellectual property. It is the aim of the paper to argue that then advertising may be included in such work.

According to Greek Law 2121/1993, the object of the right of intellectual property is the work, that is, the intellectual creation (article 1 § 1 N. 2121/93) while the subject of this right is the creator of the intellectual work (article 1§ 1, article 6 § 1 N. 2121/93). Two more rights are included in intellectual property, one of the possessive and one of the moral nature. In order for intellectual property to be substantive, such work needs to be included in material form. Two rights exist, that of work property as creation of intellect and that of proprietorship of the material form.

In article 2 §1 of Greek Law 2121/1993,

1. works of speech are associated with language symbols of written or oral speech, for example written and oral texts
2. works of art are associated with classical or modern forms such as visual or pictorial creations multidimensional, digital photographs or not, audiovisual work and expressions of modern digital communication era such as virtual reality works, video art work or multimedia -the example of the festival of video art work which has been created for advertising purposes by the International Centre of Dance in Kalamata, Greece within the framework of activities of International Dance Festival is typical for works of art described in Greek Law 2121/1993.
3. works of science are associated with individuality and a combination of form and innovation and originality as an expression of the creator.

To make a step further so as to illustrate the connection of the object of the right of intellectual property with advertising, a definition of the term originality stands in article 2 §3 of Greek Law 2121/1993: "a computer programme is considered original, since it is the personal intellectual work of its creator", a definition, though, which does not cover all the other categories. Definition is then provided in theory and regulation.

The originality of a work is consisted due to elements that elevate it to a unique and not everyday human creation as well as elements which differentiate it from existing intellectual creations and works of cultural heritage. This position is influenced by the subjective element which exists in Central European rightful system of protection and which underlines the personal bind of the spiritual creator with its work–personalised work due to personal contribution of the creator [Court of Appeals Athens 2768/2003, NoB, 2004: 51]. In the English and American system of protection of copyright, the emphasis is put on the work itself, in the sense that something different is created which has not be copied and the personal seal of the creator is not necessary [Kotsiris, 2005: 58-61; Kallinikou, 2001: 37].

Thus, it is open for discussion

a) the concept of innovation as a reference point for the protection of work especially with the technological advances and

b) the form of the work and what to include in the intellectual work creation apart from the basic categories, because every intellectual creation, if it has specific form and innovation, may be as well incorporated for protection. In that way, in the intellectual work of the law, we may include all the contemporary forms and types of work of digital era such as virtual reality works, webpages and programmes in the computer, as well as every artistic creation with the contribution of the computer, such as musical compositions, cartoon animations, digital photographs, even visual and pictorial works in digital form and others, thus, the usual content of contemporary advertisements.

The concept of the innovative work, in regard to its protection, is not differentiated from digital-communication era. In that sense, authentic is the programme in the computer and authentic is the photograph, which is the result of the personal contribution of the creator [Directive 91/250 article 3; Directive 93/98 article 6]. In regard to the form of the work, Greek Law 2121/1993 article 2 § 1 protects every innovative intellectual creation, "as is expressed in any form"and thus, the creators may express their ideas through advertising. Therefore, ideas should not be placed in blocks, they are free, such as information and is related to the inspiration and the creative capture of every artist, who will process an idea or information, offering it shape with uniquenes [Court of Athens 3859/2001: 601].

## What does US intellectual property rights include for advertising, e-commerce and what is excluded

The U.S. Copyright Act protects copyright "in original works of authorship fixed in any tangible medium of expression" [Ramsey, 2006: 199]. Under intellectual copyright property and trademark laws, advertising as well as elements of the website can be protected falling in the category of the creative content such as

1. written material which may be characterised as a literary work,
2. the layout of an advertisement, pictorial, graphic images, signs or sculptural work (e.g., illustrations, photographs, or threedimensional advertising displays),
3. musical work or sound recording (e.g., jingles),
4. or audiovisual work (e.g., commercials)
5. advertising slogans, sounds, logos, business names
6. webpages, creative website content, website designs,

7. software to create digital advertisements, such as computer generated imagery, or software including the text based HTML code used in websites and e-commerce systems,
8. search engines [Ramsey, 2006: 202; Verbauwhede, 2005: 2; Verbauwhede, 2004: 2].

Intellectual property rights for advertising and e-commerce in USA share similar issues in legislation [Verbauwhede, 2005; Verbauwhede, 2004]. There are also limits to copyright protection for advertising that exist for the US copyright law. These include the presentation of basic factual information in advertisements, such as

1. lists of goods or prices,
2. the ideas of commercial artists, such as the idea of using cartoon characters –the idea itself is not protected by copyright. Copyright only protects the expression of ideas, not the ideas themselves [Verbauwhede, 2005: 4]–,
3. or standard treatment of a particular idea and in that way it may not be considered that only one person has the exclusive right to use a specific theme for an advertising campaign or a short phrase used in advertising –[for court decisions on the abovementioned issues from USA see Ramsey, 2006: 202-204].

In that way, advertising work is considered to be intellectual property providing exclusive rights to traditional advertising or advertising over the internet offering at times more emphasis than necessary.

## The protection of the creation of advertising in EU and the case of Greece regarding advertising content

Legislation and deontology go hand in hand in many European countries as in Greece in relation to the creation of advertising messages. Regulation in advertising has many forms including regulation from the state or self regulation even if the role of state is invaluable and most professionals stick to the state regulation rather that self regulation created by themselves [Gao, 2005: 76]. At European level, harmonisation of regulation for the content of advertising creation, is imperative since markets are open for the free movement of products and people [Kavoura and Kiriakidis, 2004; Bitsani and Panagou, 2003].

TRIPS (Trade Related Aspects of Intellectual Property Rights) Treaty, is incorporated in the Final Act of the Ourougouay Round -Marakes, 1994-, which was harmonised in European countries -in Greece with Greek Law 2290/1995. This Treaty covers the intellectual property incorporating industrial and intellectual where in article 7 is mentioned that "the protection of rights of intellectual

property need to contribute to the promotion of technological advances, and the transmission and dissemination of technological knowledge in such a way so that there is mutual benefit from those who produce and use technological knowledge and social and economic prosperity is succeeded".

Advertising is finally considered to be intellectual work protected by intellectual property law as was previously described. For example, in Greek Law 2121/1993 advertising in the broad sense of "work of art" and "computer programme" is included, falling under such protection as other works do since it is the result of a creator. The harmonisation of intellectual property law in the framework of European Community with Directives was enforced in Greek legislation with Greek Law 3057/2002, article 81 with the further aim of the inclusion of the protection of intellectual and related rights in the information society.

In Greece, following and incorporating European Directives in Greek legislation, advertising is considered to be a commercial communication; entreprenual business practices towards consumers, includes every action, or way of behaving and being represented, a commercial communication, which is directly related to promotion, sales of a product to consumers [Greek Law 3587/2007, article 9a §d which amended Greek Law 2251/1994 incorporating Directive of the European Council 2005/29 and Committee EE L 149].

European Directive 89/552/EEC of the Committee of the European Communities of 3.10.89, as this was amended with European Directive 97/36/EK of the European Parliament and the Council of European Union concerning radiotelevision activities was incorporated in member states' legislation. In Greece, harmonisation exists with the Greek Presidential Decree 100/2000 following European Directives and legislation so that Greek legislation acts in accord with them. The Greek Presidential Decree 100/2000 covers the legal framework within which the content of advertising communication is created (article 2§c, d, e) so that the creation of misleading, unfair, or comparative advertising is avoided.

In addition, Directive of the European Parliament and the Council 2006/114/EC 12.12.2006 concerning misleading and comparative advertising replaced Directive 84/450/EC on misleading advertising and codifies the amendments made to Directive 97/55/EC which included comparative advertising. This Directive essentially has effect from 12.12.2007 from member states for their policy and legislation.

The abovementioned legislation refers to misleading advertising which includes false or not true information as a whole regarding the product and its characteristics while it may be also manipulative when it is contrary to the demands of professional deontology; comparative advertising as the one which implies the iden-

tity of the competitor, yet, the creation of such advertising may be allowed when this is done in an objective way for more than one characteristics of a product and does not aim to the depreciation of trademarks or the name of the competitor. Directive 89/104 EEC approximated the laws of the member states relating to trademarks.

Those involved with the implementation of the advertising campaigns need to be aware and become familiar with the legal advertising framework for the best possible adjustment of advertising messages in society and the avoidance of the creation of an advertising communication programme of a business or of a cultural organisation which does not pay attention to the legal requirements created for the protection of the business sector and the consumers.

Advertising may be also in control within the framework of self-regulation from the field of advertising itself and the agencies and committees control, such as the German advertising Council (Werberat) [Kroeber-Riel, 1998: 60] or the Council of Control for Communication for Greece created by the Committee of Greek Advertising Agencies and enforcing the Greek Code of Advertising-Communication [http://www.edee.gr]. This is a Code which was initially enforced voluntarily then was legally established and which incorporates rules that are associated with the way communication ought to be promoted [Kavoura, 2008].

## Who is entitled to the intellectual property for the creation of advertisements according to legislation?

The legal protection of intellectual property in European Union came from the law for the protection of industrial and commercial property.

In the beginning, the term intellectual property was not in the text of the Treaty of Rome for the European Community (EC) and was harmonised in Greece with Greek Law 2054/1992. In the passage of time, the Court of the European Communities [Cotidel v. Cine' Vog Films S.A. 62/79; Musik Vertrieb Membran et K. Tel/GEMA 55-57/80] judged that in the article 36, already article 30 of the EC, "industrial and commercial property" intellectual property needed to be included. In that way, intellectual property was incorporated in the original legislation. The economic importance of intellectual rights and the initiatives of USA in copyright issues led the European Community to create Directives. This harmonisation effort begins from the Community and the Green Book of 7/6/1988 leading to 8 Directives so far which comprise of a solid cell of legislation, as is property part of which is intellectual property [Kotsiris, 2005].

The costs of intellectual property protection normally include transaction costs, rent seeking, and enforcement costs. Copyright vests initially in the author or au-

thors of the work. The author of the work is the person (or persons) who created the expression in the advertising, unless the advertising is a work made for hire.

Other times advertising departments of advertising agencies, hire free lancers to plan, create, and communicate their advertising while if advertising messages are created by employees who work in advertising agencies, the employer has the copyright in the advertising unless another agreement has been signed.

As far as the advertiser and the advertising agency is concerned in regard to ownership of copyright in the advertisements, the agency retains copyright in the creation of advertising [Ramsey, 2002: 13-14]. Whichever is the case, contracts safeguard all the involved sides. Then, issues related to bullying the work place is safeguarded because there is beforehand agreement on the rights and responsibilities of the parties involved (Kiriakidis and Kavoura, 2005).

The example described below illustrates that contracts may actually define each specific case. The example is from the Hellenic Organisation's of Tourism International Analytic Invitation in 1997, Directorate of Advertising, Public Relations in regard to the creative printed material (photographic and artistic) that would be created by an advertising agent. The Hellenic Organisation of Tourism asked that this material would be its property and may be used whenever needed. Intellectual and related rights for the use in any way from the Hellenic Organisation of Tourism will belong to it and the advertising agency will resign the rights [Kavoura, 2006].

## Conclusion

Management of content and information in a digital environment [Bottis, 2004b] is an issue that is very much associated with the content of advertising messages. Freedom of expression should not be constrained from legislation regarding the content of advertising which aims to promote and disseminate information as much as possible regarding a product or service regardless of copyright protection. Freedom of expression in advertising communication is a necessity to exist yet, control mechanisms safeguard justice and equality for all.

That is why, examination of the way the content of advertising messages are created needs to be continuously evaluated since changes follow society and society needs to follow changes. The person in charge of the creation of advertising communication, should be aware of copyright issues and legislation regarding the way advertising content is defined in order not to create misleading, comparative or unfair messages or even depreciating trademarks of competitors. In order not to reach courts and deal with legislation, contracts need to take place (Varka-Adami, 1995). Effort should be continuously made for the best possible presen-

tation of advertising messages, respecting the consumer, the competitor, society, the creator, within a legal framework in the information age.

## References

Barka, Adamh, A. (1995), Civil Law, (2nd ed.), Sakkoulas, (in Greek).

Balasubramanian S., Karrh J., and Patwardhan H. (2006), Audience Response to Product Placements, An Integrative Framework and Future Research Agenda, Journal of Advertising, 35, 115-141.

Bitsani E. (2004), Culture Management and Regional Development. Culture Policy Planning and Cultural Product Planning, Athens, Dionicos, (in Greek).

Bitsani E. and Panagou V. (2003) Local media, local government and culture, *Applied Research Review*, VIII, 1: 165-176.

Bottis M. (2004a), A Different Kind of War: Internet Databases and Legal Protection or how the Intellectual Property Laws of the West Threaten the Developing Countries' Information Commons, International Journal of Information Ethics, 2 online at http://papers.ssm.com/sol3/papers.cfm?abstract_id=952882 accessed 10.04.2010.

Bottis M. (2004b), The Law of Information- Issues of Intellectual Property, Patent, Librarianship and Advertising, Nomiki Bibliothhiki (in Greek).

Bottis M. (2003), Tort Law Hellas, Kluwer Law International, International Encyclopaedia of Laws, online at http://untreaty .un.org/ilc/documentation/english/a_cn4_543.pdf accessed 06.04.2010

Chung E., Hwang H., and Kim M. (2007), Evaluation of non-English dietary supplement advertisements in an ethnic minority community in America, Public Health Nutrition, 10, 834-837.

*Cotidel v. Cine' Vog Films S.A. 62/79*

Drumwright M., and Murphy P. (2004), How advertising practitioners view ethics. Moral, Muteness, Moral Myopia and Moral Imagination, Journal of Advertising, 33, 7-24.

Gao Z. (2005), Harmonious Regional Advertising Regulation? A Comparative Examination of Government Advertising Regulation in China, Hong Kong, and Taiwan, Journal of Advertising, 34, 75-88.

Kallinikou D. (2001), Intellectual property and Internet Directive 2001/29/EK, Sakkoula (in Greek).

Kavoura A. (2008), Advertising communication and the legal framework in the creation of Greek advertisements, Issues of Communication, 8, 28-45 and online at http://www.media.uoa.gr/institute/pages/gr/zitimata_gr.html accessed 12.4.2010.

Kavoura A. (2006), A critical approach of the rules of transparency in the media relations with the advertising agencies: examples from the field of tourism, Tourism Scientific Review, 3, 3, 9-27 and online at www.traveldailynews.gr/pdf/Epth3/AndronikiKavoura.pdf accessed 14.4.2010

Kavoura A. and Kiriakidis S. (2004) Points of interest in the creation, transmission and advertising control, Media and Communcation (Dikaio ton Meson Mazikhs Enhmeroshs kai Epikoinonias, 4, 502-504 (in Greek).

Kiriakidis S. and Kavoura N. (2005) Bullying in the workplace: current empirical findings and suggestions for future research, Business and Economy, 2, 135-147.

Kotsiris L. E. (2005), Intellectual Property Law, (4th ed), Sakkoula (in Greek).

*Musik Vertrieb Membran et K. Tel/GEMA 55-57/80.*

Kroeber-Riel W. (1998), Strategy and Technique of Advertising, Ellinika Grammata (in Greek).

Ramsey L. P. (2006), Intellectual Property Rights in Advertising, Michigan Telecommunications Technology Law Review, online at http://www.mttlr.org/voltwelve/ramsey.pdf accessed 06.04.2010

Ramsey, L. P. (2002), IP Ownership: Avoiding Disputes, WIPO Magazine, Nov-Dec, 13-15 online at http://wipo.int/sme/en/documents/wipo_magazine/11_2002.pdf accessed 11.4.2010.

Russell A., and Belch M. (2005), A Managerial Investigation into the Product Placement Industry, Journal of Advertising Research, 45, 73-92.

Russell C., and Stern B. (2006), Consumers, Characters, and Products. A Balance model of Sitcom Product Placement Effects, Journal of Advertising, 35, 7-21.

Spinello R. & Bottis M., (2009) A defense of intellectual property rights, Edward Elgar Puplishing.

Thlikidou-Stogianni, E. (2003) Post-modern Marketing: review, University Studio Press (in Greek).

Verbauwhede L. (2005), Intellectual Property Issues in Advertising, World Intellectual Property Organisation, online at http://.www.wipo.int/sme/en/documents/ip_advertising.htm accessed 06.06.2010

Verbauwhede L. (2004), Intellectual Property and E-Commerce: How to take care of your Business Website, World Intellectual Property Organisation, September 23, online at http://.www.wipo.int/sme/en/documents/ip_advertising.htm accessed 06.04.2010

Zotos G. (2008), Advertising, Design, Development, Effectiveness, (5th Ed), Thessaloniki: University Studio Press (in Greek).

# Illegal downloading: proposed solutions from the EU member states

Galateia Kapellakou

## Introduction

The technological evolution and the dissemination of the works in the digital environment have put into doubt the traditional copyright system. The question that arises is whether the rights of the author as regulated by the current intellectual property system a re effective in the digital environment, especially as far as digital recording and transmission process, satellite communication and the Internet is concerned.[1] In this context, copyright theory does not share the same opinion on how Copyright should react to the Internet revolution.

*Grosso modo*, current copyright theory can be divided into three groups: the neoclassics, the minimalists and the eclectics (elitists). The neoclassics consider that copyright as organised today is perfectly capable of confronting the economic exploitation of works on the Internet. This theory sustains that the problem is that the Internet and the new methods of exploitation and dissemination harm the existing relative industry and may provoke its disappearance if the rights of the authors are not protected more intensively.[2] Thus, if some updating is needed in the digital environment, this is in order to reinforce the position of authors and to enhance their rights in the digital environment. On the other hand, the minimalists are opposed to the expansion and reinforcement of the rights of the authors in the digital environment and are interested in reducing Copyright's power in favour of the users.[3] According to this theory, access to the works is almost annihilated because of the application of the rights to the mere use of works and the restriction of exceptions and limitations. Finally, the eclectics (elitists) seek to reach the reasonable equilibrium between the rights of the authors and the abilities offered to the users by the digital environment. This theory seeks to adapt the rights of the author in order to answer to the new necessities.[4]

In our view, the reaction to the dissemination of the works without authorisation is legitimate and imperative. Copyright is the most efficient method to finance intellectual creation. The remuneration of the author is the incentive that urges him to create and at the end, promotes the cultural development of each country. Thus, remaining passive to illegal downloading is not an option. This anomalous situation can be treated in two ways: prevention or repression. Though the first

way seems to be the most adequate solution, we doubt whether the proposed solution by the EU member states can be classified under the preventive measures.

Before entering into the core of the proposals and express our scepticism on the efficiency of these measures, it is interesting to note that downloading and peer-to-peer file sharing is not treated in the same way in the Member States. The first question that should be answered is which rights are involved in the digital transmission and then focus on the system model a legislator should follow in order to eliminate illegal downloading. Thus, before analysing the systems proposed by the EU member-states (paragraph 2) it is interesting to examine the notion of downloading and the Peer-to-peer file sharing system (paragraph 1).

## *Downloading and peer-to-peer file sharing*

Though 14 years have passed since the WIPO Copyright Treaties[5] were adopted and almost ten since the Information Society Directive[6], theory is not consistent regarding the interpretation, application and breadth of copyrights[7]. I also doubt that there is an actual harmonisation within European Union. Member-States and national judges do not respond in the same way to the new technology, while, as far as their effectiveness is concerned, the facts show that one should be sceptical.

Downloading, according to the standing legislation, is a reproduction. It is important however to understand that downloading does not imply only permanent reproduction, meaning downloading that will be stored on the hard disk of the computer, but any form of downloading, even temporary. Since the Information Society Directive regulated that reproduction comprehends direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part (article 2), there is no doubt that reproduction can be found even in the streaming technology that transmits the work in real time. Thus, the user who receives a work in streaming without authorization is infringing both the reproduction and the communication to the public right and cannot be excused by the (obligatory) exception set in article 5§1 of the Information Society Directive[8] because of the unlawful character of the use. Nonetheless, part of the European doctrine seems hesitating on the amplitude of the reproduction right. It is true that this expansion of the reproduction right complicates economic rights, while it is considered –by some authors- to unjustifiably expand the rights of the author and creating an access right.

The problem in my opinion is that, Member States, when proposing for solutions in order to combat Internet infringement of Copyright, have in mind the illegal peer-to-peer file sharing as it operates today, though downloading and file sharing does not pass necessarily by storage. The peer-to-peer system work as follows.

The computers use a software which enables them to "communicate" and their users (or "peers") to upload, search for, access and download material stored in "shared" files on the computers' hard drive[9]. When someone is downloading (in P2P systems) he is actually retrieving all or part of the content he wants, whether from a peer or a server. When uploading, the user is sending all or part of a content (file) to other users. In order to upload a permanent reproduction is necessary. The techniques of peer-to-peer allow the download and upload simultaneously, meaning either the downloading/uploading of several content or of the same content: as part of a shared content is downloaded, it is immediately available for upload.[10] The actors involved in P2P file sharing are a) the one that makes the upload, thus reproduce permanently the protected work and makes possible to other users (peers) to access it, b) the one who access and downloads the work, c) the operator that provides the software that enables the peer-to-peer file sharing and d) the ISP.[11]

Uploading is definately illegal. Regarding downloading, theory is not unanimous whether downloading in P2P file sharing systems should be considered as private copying or not. In France, court decisions consider downloading illegal relying on the fact that the condition of the legality of the source of the copy is not met[12]. However, the doctrine seems sceptical on the importance of this condition, since in order to apply the private copy exception what is important is that the use of the work is strictly private[13]. In the P2P case the problem is that the one who downloads is –in some cases- at the same time uploading for someone else. But even if we consider that P2P file sharing is private copying, the exception could not apply because of the three-step test.[14]

Yet, one should also take into consideration that the streaming technology is going to change the way that P2P works. P2P file sharing is popular because of Internet low-speed connexion (it allows downloading the same file from several users simultaneously). As soon as the speeds of Internet connection become high, the users will turn to streaming techniques. In the case of streaming, no permanent downloading is required since the work is transmitted in real time. Data are normally transformed into pictures or sound automatically. Only in some cases data exceed the permitted volume and must be temporarily (not permanently) stored in a "buffer". The question is whether "downloaders" who stream copyright material infringe copyright. Supposing that these "streamers" do not upload at the same time protected material they should not be found liable for illegal reproduction, unless one considers that the temporary reproduction effectuated in this case does not fall under the obligatory exception of article 5§1 of the Information Society Directive.[15] But neither does this question receive a unanimous answer by the doctrine. Of course, the simple answer to this is that in any case

the three step test will not permit such a use and, thus, the exception becomes ineffective.

The actual problem is that once P2P starts using streaming technology and works are exchanged directly between peers (from one user to another) in streaming it will not be easily detected the IP address because there is no server involved.[16]

## Proposals

### *Three-strikes system*

### France - HADOPI[17]

The French proposal is the one that has been discussed the most. By this initiative called HADOPI or "reponse penal gradue" the French legislator aimed to incriminate those Internet users that participated in the exchange of protected material through P2P systems.[18] In reality this provision relies on a breach of an obligation to survey the access to internet that enabled the infringing act and not to the mere act of infringement.[19] This obligation imposes to the person that has access to online communication to the public services to "to ensure that this access is not being used for reproduction, representation, or making available or communication to the public of works or objects protected by copyright or a related rights without the permission of rights holders (...) when this permission is required." This system aims at the prevention and regulation rather than the repression of abusive users. Besides civil and penal procedure the text introduces and organises in case of misuse (infringement) a mechanism that will punish any lack of surveillance for which the holder of the access is considered to be responsible.

The Constitutional Council censured some parts of the HADOPI as contrary to the French Constitution.

HADOPI is actually confided to a commission of three "magistrates" appointed by a decree that could not be revoked or renewed beyond six years. The magistrates were entitled to decide between 1) the suspension of the access to the internet for two months to one year while at the same time the infringer could not subscribe to another service provider or 2) an injunction to take, within a specific time limit, some measures capable to prevent the repetition of the violation by apposing one of the security software provided by the list that had been published by HADOPI.

The Constitutional Council ruled that access to the Internet is part of the fundamental right of the freedom of expression and communication. Even though the right should co-exist peacefully with the other constitutional freedoms (here the property right), the administrative penalty, imposed by an independent administrative authority that has no judicial competence, is not different to a penal sanc-

tion. However, it should be noted that the actual problem was not that the decision was made by an administrative authority but the fact that freedom of expression and communication are rights of such a particular nature that any measures taken should be necessary, adapted and proportionate to the objective pursued. The Council considered, thus, that in this case the magistrates had a very large domain of competence which could not be considered as proportionate.

The Constitutional Council also found that the HADOPI infringed the presumption of innocence. The law provided that, in case of fraud or *force majeure*, no sanction could be taken against the subscriber who had apposed the security means provided by the relevant HADOPI list. At the same time, the burden of proof was reversed: that the subscriber has to prove exemption from liability. Such a presumption, according to the Constitutional Council, could be valid only if the presumption did not have irrefutable character, the right of defence is respected and the facts reasonably induce probability of liability. The problem was also that the subscriber should prove not only that he is not the one who committed the infringement but also that someone else had used his IP address which is quite difficult knowing that pirating an IP address is not that difficult. Furthermore, the reverse of the burden of proof equates to a presumption of culpability, which is contrary to the Constitution.

Nevertheless, the Constitutional Council did not censure the sending of warning notices to the subscribers, thus, it validated the Commission's capability to process the subscriber's personal data. The HADOPI project modifies Article (L. 34-1) of the "Code de postes et telecommunications electroniques" and the ISPs will have to keep data for one year so that the Commission can find users who have not surveyed adequately their Internet access. The Commission will receive the IP addresses and any other relevant document and information such as the identity of the user, his regular address, his electronic address and his phone number. The Constitutional Council, in order to ensure a balance between privacy and other rights, admitted the possibilities for the collecting societies to effectuate the process of personal data related to copyright infringement, under the condition that the data will acquire a personal character only in the context of legal proceedings and under the condition that the process of personal data will be authorized by CNIL (Commission Nationale de l'Informatique et des Libertés).

The censure of the Constitutional Council did not deter the French Legislator from proposing HADOPI 2 that conforms to the Council's censorship and has been adopted by the Senate (July 2009) and the Parliament (September 2009).

The magistrates still have the power to suspend the internet access of the user in case a) a copyright infringement occurs and b) the user did not secure the Internet access. Infringement of copyright can lead to 3 years imprisonment and a

penalty of 300.000€ that has already been provided under art.L.335-2, L.335-3 and L.335-4 of the CPI but complementary the suspension of the Internet access for a period of maximum 1 year pronounced by the magistrates of HADOPI. The infringer has still the obligation to pay the Internet provider even though he is disconnected or if he wants to break the contract, he should encumber the costs. The Internet user that has been disconnected is not allowed to subscribe under a new ISP and in case this happens there is a risk of two years imprisonment and 30.000€ penalty. However, the complementary penalty of the law HADOPI must be decided by judges of the judicial authority. A simplified, accelerated, written and not adversary procedure will be followed (provided under the penal law in art. 495) by criminal courts consisting by one judge. This judge will have the power to decide the interruption of the Internet access for a maximum period of one year, without the Internet user been heard. The user whose connection has been interrupted will be able to react within 45 days.

## UK - Digital Economy Bill

In the UK discussions cover the responsibility of ISPs in the context of "survey and suspension of services". The first signs of the British response to the illegal downloading can be found in the Digital Britain Report published last year (June 16, 2009) by the Government[20]. As far as illegal downloading is concerned, the British Report[21] - which also refers to the peer-to-peer file sharing as the major concern for the content industries, proposes a process in two stages. It recognises Ofcom[22] as responsible for the enforcement and the reduction of copyright infringement. It gives the power to Ofcom to oblige ISPs to "notify account holders on receipt of appropriate evidence that their account appears to have been used to infringe copyright and maintain and make available (on the basis of a court order) data to enable the minority of serious repeat infringers to be identified."[23] The report is also proposing the adoption of an ISP Code[24] that sets the obligations of the ISPs. In case the admittedly dificult target of 70% reduction of copyright infringement is not met, the report proposes that Ofcom will be able to impose to ISPs the use of technical measures such as "a) blocking content, either particular websites or protocol blocking to deny access to particular services, b) reducing the speed or volume of data downloaded by bandwidth capping (which caps the speed of a subscriber's, internet connection and/or caps the volume of data traffic which a subscriber can access) and bandwidth shaping (which limits the speed of a subscriber's access to selected protocols/services and/or caps the volume of a data to selected protocols/services), and c) content identification and filtering."[25] As it is understood, the British report does not propose the disconnection as a penalty. This is the most important difference between the French and the British proposal.

Following the Digital Britain report the Digital Economy Bill was announced on 18 November 2009 and had its Second reading on December 2009.

According to the Bill, the two stages of the procedure remain as proposed in Digital Britain Report. The first stage provides for two initial obligations by the ISPs. ISPs are obliged to send letters to users, subscribers who have been found to infringe copyright and in case of repeated copyright infringement, they will be required to collect information on infringers that will be handed out to copyright owners but the identity of the infringer shall not be revealed unless there is a court decision.[26] The proposal of a Code of Practice is also part of the bill. This Code, that is supposed to be drafted by Ofcom after consultation, will actually be an agreement between the parties involved (meaning the ISPs, the copyright holders and consumers).[27] Ofcom will also have to prepare (full and interim) reports that will state the progress of fighting against internet infringement of copyright in order to assess the effectiveness of the measures.[28]

The Bill also provides for obligations on limiting internet access as proposed in the Digital Britain Report (technical measures that will "limit the speed or other capacity of the service provided to a subscriber, prevent a subscriber from using the service to gain access to particular material, or limit such use, suspend the service provided to a subscriber, limit the service provided to a subscriber in another way.")[29] The Code will also regulate the limiting of internet access and must set down the procedure when the user wishes to appeal to the imposition of technical measures that restrict his access to material available on Internet.[30] In case ISPs do not comply with the obligation to limit the access, Ofcom is entitled to set a penalty of maximum 250,000 euros. The costs of the notifications are shared between the rights holders and the ISPs (flat fee for the rights holders for each notification that will be calculated on the cost that encumbers the ISP in order to process the notification).

## Ireland

The only member state that has actually applied the three-strikes "method" is Ireland. However, no relevant Statute has been adopted or proposed by the Irish legislator and the three-strikes systems is applied only by one telecommunications company.

What has actually happened is that the ISP that holds the biggest part of the Irish telecoms market reached an out-of-court settlement in February 2009 with the Irish Recorded Music Association (Irma) (EMI, Sony, Universal, Warner etc) Under this agreement, the telecoms company agreed to introduce the graduate response system. Actually, the provider will suspend the internet service for the internet connection of those users who are repeatedly sharing music. The High

Court in Dublin (16th of April 2010), ruled that an IP address is not personal data in this specific case, approving, thus, the agreement and permitting the implementation of the settlement.[31]

Infringing customers will on the first strike be reached on the phone in order to be informed on their illegal activity. In case the user is identified to infringe for a third time, the company will send *a termination notice and, subject to extenuating circumstances arising the user will be disconnected thereafter. D*isconnections, however, are supposed to be carried out when the company is certain that there is an infringement and that the user had the opportunity to explain its circumstances and that there is no fraud in the detriment of the user.

## "Softer" systems

### *Spain – Project of Economic Sustainability*

The Spanish legislator decided not to follow the three-strikes system and instead of punishing the public that accesses and downloads the illegal content, he is turning to the responsible parties of the websites that make available the protected material (with or without knowing it). The proposed solution was announced by the Project of the Law for Economic Sustainability[32] and seems must softer that the three-strikes system. However, it is not certain if it is going to have the desired results –Spain is the European country with the most illegal downloads- especially when blocking a website is not something new. This draft law manages only to reduce the duration of the procedure.

The process of blocking a website starts when the rights holders complaint to the Commission that a web page is storing, making available or linking to protected material without authorization. The Commission then checks if there is actually an infringement and -if this is the case- notifies the web administrator over the complaint and gives a time-limit to party responsible of the website in order to present his arguments. If these arguments and are rejected, the Commission notifies the party responsible of the website that the infringing files that are the object of the unlawful use should be removed and designates the period in which the content should be removed.

If the web administrator does not remove the infringing content then -and only then- it is possible to ask for precautionary measures on Court. These measures are the interruption of the service provision or the data storage in case of a national site or the blocking of foreign Web sites with illegal content. This blocking will be carried out by national operators of Internet access.

The judge does not enter into the merits of the case, but may decide whether the Commission is competent to close the site or not and if the measure taken

by the Commission conflicts with fundamental rights (such as the right to information or freedom of expression). This judicial phase is supposed to last less than a month. Ordinary legal proceedings in order to examine the merits of the case may be asked by each party.

### *Sweden – Development of digital services & public awareness campaigns*

Sweden preferred the more debatable way to fight against piracy, but surprisingly it seems that it is working. Instead of turning to solutions such as the three-strikes, "Sweden's resurgence appears to show a combination of the carrot of music offerings and the stick of the new enforcement legislation"[33]. Thus, the Swedish campaign that informed the public on the new law (implementation of the Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights)[34] along with the development of user-friendly digital services had as a result the increase of the digital sales in Sweden. Of course, one should keep in mind that public awareness campaigns[35] do not have the same effect in all the member states, even when user friendly digital services are offered.

## EU level

After having exposed our doubt on the harmonisation of the economic rights at European level concerning the effectiveness of the economic rights as set by the Information Society Directive, we will try to understand towards which direction European Commission is moving.

First of all we must refer to the issue of personal data which seems to be quite delicate for the European Court as it hesitates to give a definitive answer on this matter. The ECJ refused to uphold a decision when it was asked by the Commercial Court of Madrid (preliminary ruling) whether an (ISP) is obliged in civil proceedings to disclose the identities of people allegedly infringing copyright by illegally downloading content. The ECJ held that nothing in the wording of the European Directives required that they must be interpreted as forcing Member States to lay down such an obligation and pointed out that the Directive 2004/48 specifically provides that efforts to ensure effective protection of copyright apply without prejudice to statutory provisions that govern the protection of confidentiality of information sources or the processing of personal data.[36]

Thus, the ECJ did not change the status of the ISPs nor did it rule in favour of the IP rights holders. We will have to wait either for another decision in order to understand whether the ISPs safe harbour is going to change or for the European legislator to adopt a new directive that will deal with personal data in the field of IP or the change of the status of the ISPs.

Secondly, the Gallo report 2010[37] on the enforcement of intellectual property rights in the internal market, prepared by the Commission and adopted in the JURI committee of the European Parliament on the 6th of June, gives some information on the position of the EU concerning illegal downloading and generally Internet infringement. In order for the EU to eliminate unlawful downloading, it is not impossible to see the enforcement directive amended. EU seems to be open to any solution that would have as a result the development of the European digital market and the creation of a legitimate online market.

Although this report does not give specific information on how illegal downloading is going to be treated at a European level, whether the ISPs safe harbor is going to be preserved or whether the personal data legislation is going to be modified, some parts of the Parliament's proposal are worth to mention.

After admitting that the unauthorized file sharing is a problem that affects the European economy in terms of job opportunities and revenues for the industry as well as for government[38], the Parliament expresses its regret "that the Commission has not mentioned or discussed the delicate problem of online IPR infringements, which constitutes a major aspect of this worldwide phenomenon in the age of digitisation of our societies, particularly the issue of the balance between free access to the Internet and the measures to be taken to combat this scourge effectively urges the Commission to broach this problem in its IPR strategy"[39] The Parliament then stresses out the necessity to develop in European level "a diversified, attractive, high-profile, legal range of goods and services for consumers" recognising that a functioning internal European digital market should be developed or else it will not be possible to create a legitimate online market[40]. It also points out that an appropriate solution must be found (all parties involved should participate in the dialogue-stakeholders and ISPs) or else the Commission should consider a legislative proposal or the amendment of existing legislation, (particularly Directive 2004/48/EC), so as to upgrade the Community legal framework in this field on the basis of national experiences.[41]

## Conclusion

Governments have to choose between the political costs of adopting a three-strike system while at the same time, lobbies are pressing for action pointing out that the economic loss of the cultural industry affects the national economy and the cultural development.

Should the peer-to-peer file sharing be one of the most important issues of the proposals from the EU member states, one should not forget that illegal downloading is not found only in peer-to-peer systems but also in temporary reproduction that is necessary for example in streaming technology too. One should

also have in mind that the way file sharing is operating today is going to turn to streaming technology, in which case it is not easy to detect the assumed infringers or to other technologies such as Bluetooth.

The proposals do not take into consideration systems working on friend-to-friend scale, either. "Such a system works, as its name indicates it, between friends, or at the most by a mechanism of invitation. Networks, are organized around communities in which communications are private, preventing any control of the exchanged data. Investigations within such networks to notice infringements of rights literary and artistic property require considerable means of intervention and infiltration inside "friends' networks" which exchange protected works."[42] Supposing that national commissions start sending notices to these users, the result will be that the members of these networks will abandon the "community". This is not impossible to be found as harming freedom of expression (these social networks do not aim at copyright infringement).

In our opinion, whether a system chosen to eliminate illegal downloading is going to be effective or not, does not depend only on the strictness of the law or the willingness of the Member-States to enforce the law. The possible reluctance of the citizens to abide might lead to rethinking the model Europe is following. We share the same opinion with professors Vivant and Bruguière that the three-strike system, "is finally more severe than the actual one. Under the guise of prevention, the legislator would hold a collective punishment mechanism via an administrative authority. An insidious decriminalisation because repression would finally be harder…"[43].

Many studies have been conducted on the matter of illegal downloading and unlawful file sharing providing for alternative solutions as far as the remuneration of the author is concerned (without depriving him from the exclusivity of his rights) or how legalisation of peer-to-peer file sharing could be in accordance with the *droit d'auteur* system.[44] Isolated reactions of the Member-states are, in our view, condemned not to last. The word frontiers is difficultly applied to the digital environment.

## Endnotes

1. J.A. Sterling, The Future of Copyright: Approaches for the New Era, An address to the British Literary and Artistic Copyright Association, London 12 March 2009, available on line: http://www.blaca.org/meeting2009.htm.
2. Ignacio Garrote Fernández-Diez, El derecho de autor en Internet, Editorial Comares, second Edition, Granada 2003, p. 65-66. The neoclassic theory is examined more thoroughly in pages 66-79.
3. Ibid, p. 66 and more thoroughly p. 79-90. According to the author, this theory is further divided into radical liberalists that –more or less- doubt copyright's justification, and the democratic minimalism according to which internet gives the opportunity to the citizens to participate to the democratic dialogue and to the decision making process, which applied

in copyright means that each member of the public can participate in the creative process (derivative works).

4. Ibid p. 66, more thoroughly p. 90-101. This theory is divided, according to the author, in two categories: the first equals information and work and refers to the right of information and the second (that is in favour of the evolution of copyright and its flexibilisation) refers to the historical analysis of this branch that shows that copyright has always adapted to technological evolutions.
5. Adopted in Geneva on December 20, 1996 (WCT).
6. 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.
7. On a description of the debate for and against intellectual property rights see Spinello R. & Bottis M., A defense of intellectual property rights, 2009.
8. Art. 5 §1. "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."
9. Haflidi Kristjan Larusson, "Uncertainty in the scope of copyright: the case of illegal file-sharing in the UK", E.I.P.R. 2009, 31(3), 124-134 (124).
10. Franck Macrez & Julien Gossa «Surveillance et sécurisation: ce que HADOPI rate» RLDI -2009, N°50, 50-41 (§26).
11. Haflidi Kristjan Larusson, "Uncertainty in the scope of copyright: the case of illegal file-sharing in the UK", E.I.P.R. 2009, 31(3), 124-134 (124).
12. See Mulholland drive case, Cour de Cassation, civ.1, 19 juin 2008, M. Perquin, UFC Que choisir c/ Soc. Universal Pictures Vidéo France et a.
13. Michel Vivant & Jean-Michel Bruguiere, Droit d'auteur, DALLOZ, First edition, 2009, p. 400-401 § 591.
14. An analysis on how downloading from P2P systems when there is no uploading at the same time passes the three step test see Nantes report prepared by Carine Bernault & Audrey Lebois,

    Under the supervision of Professor André Lucas ("By the Institute for Research on Private Law, University of Nantes), "Peer-to-peer File Sharing and Literary and Artistic Property, A Feasibility Study regarding a system of compensation for the exchange of works via the Internet, June 2005, avail. http://privatkopie.net/files/Feasibility-Study-p2p-acs_Nantes.pdf. Generally about the interpretation of three step test see, "Declaration: a balanced interpretation of the three-step-test in Copyright Law", Max Planck Institute, available at http://www.ip.mpg.de/shared/data/pdf/declaration_three_step_test_final_english.pdf.
15. For the British doctrine the question is whether buffering is a substantial copy of the work: "Storing temporary copies in the computer's buffer constitutes "copying" under s.17(6) of the CDPA, which states that "[c]opying in relation to any description of work includes the making of copies which are transient […]". Therefore, the issue here is not whether buffering leads to copying, but whether it is copying of "a whole or any substantial part" of a copyright work, as

required by s.16(3)(a) of the CDPA." Haflidi Kristjan Larusson, "Uncertainty in the scope of copyright: the case of illegal file-sharing in the UK", E.I.P.R. 2009, 31(3), 124-134 (127).

16. Liul Y., Guo Y. et Liang C., «A survey on peer-to-peer video streaming systems» in Peer-to-Peer Networking and Applications, Springer New York, 2008.
17. Articles relevant to HADOPI (indicative): Jean-Michel Bruguière, Loi «sur la protection de la création sur internet»: mais à quoi joue le Conseil constitutionnel ?, Recueil Dalloz 2009 p. 1770/Laurent Szuskin, «Sans contrefaçon» ? Une étude comparée de la lutte contre le piratage en ligne des droits d'auteur et voisins, RLDI, N°50, 2009/Franck Macrez & Julien Gossa «Surveillance et sécurisation: ce que l'Hadopi rate», RLDI N°50, 2009/Asim Singh, «Le streaming et la loi «Création et Internet», RLDI - N°50/Mathieu Coulaud, «L'adoption au Sénat du projet de loi «Création et internet»: la confirmation d' une méthode de régulation consensuelle en propriété littéraire et artistique», RLDI, N°46, 2009/Allan Gautron, «La «réponse graduée» (à nouveau) épinglée par le Conseil constitutionnel», RLDI 2009, N°51/ Bruno Dreyfus, «Quelle est la nature de la mesure de suspension de l'accès à internet prévue par le projet de loi «Création et Internet» ?», RLDI 2009, N°49/ Hubert Bitan, «Réflexions sur la loi «Création et Internet» et sur le projet de loi «HADOPI 2», RLDI, 2009, N°51/Éléonore Mirat & Patrick Boiron, RLDI 2009, N°51, «La loi HADOPI: beaucoup de bruit pour rien ?»/Iliana Boubekeur, «De la «loi HADOPI» à la «loi HADOPI 2»RLDI - 2009, N°51, 51-57/ Marc-Antoine Ledieu, «Le projet de loi HADOPI adopté», Communication Commerce électronique n° 6, Juin 2009, alerte 75/Christophe Caron, Le Conseil constitutionnel au secours de la rémunération pour copie privée, Communication Commerce électronique n° 6, Juin 2009, comm. 54 etc.
18. Michel Vivant & Jean-Michel Bruguiere, Droit d'auteur, DALLOZ, First edition, 2009, p. 736-737.
19. Iliana Boubekeur, «De la «loi HADOPI» à la «loi HADOPI 2», Revue Lamy Droit de l'Immatériel (RLDI) - N°51, 2009.
20. According to the report, as more and more vital services, including education and health, will be delivered solely online in the future, the Government makes one of its main policy aims, to increase "affordability, capability and availability" of digital technology such as the internet. See Katrina Dick, "Digital Britain - a summary", Ent.L.R. 2009, 20(8), 283-286 (283).
21. Which "met with criticism from opposition politicians and the media for inaction on securing the swift and wide deployment of next-generation networks that is being witnessed in some other countries", Bailey Ingram & Paul Brisby, The Digital Britain White Paper, C.T.L.R. 2009, 15(7), 151-153.
22. Ofcom is the communications regulator that regulates TV and radio sectors, fixed line telecoms and mobiles, plus the airwaves over which wireless devices operate. Ofcom operates under the Communications Act 2003. The Act provides that Ofcom's general duties should be to further the interests of citizens and of consumers. Meeting these two duties is at the heart of everything we do (http://www.ofcom.org.uk/what-is-ofcom/).
23. Katrina Dick, "Digital Britain - a summary", Ent. L.R. (Entertainment Law Review) 2009, 20(8), 283-286 (283).

24. Ibid, "setting out how ISPs should comply with this new regime, including practical measures, appeals, standards of evidence and the apportionment of costs. It is envisaged that Ofcom will have the power to fine ISPs and rights holders for failing to comply with the code."
25. Carolyn Burbridge, Graeme Maguire, Digital Britain – the final report, Computer Law & Security Review 25 (2009) 482 – 484.
26. The Explanatory Notes propose a definition of serious repeat infringer, e.g. as someone who has received 50 copyright infringement reports. See Florian Koempel, Legislative Comment, DIGITAL ECONOMY BILL, C.T.L.R., 2010, 16(2), 39-43 (40).
27. This Code is supposed to: a) "cover the procedure of this process, detailing among others: the way copyright owners detect copyright infringement; standard of evidence to be submitted to ISPs in a copyright infringement report; appeal mechanism" and b) "specify the notification obligation, including: description of apparent infringement; information on the purpose of copyright; advice on legal sources for copyright content; advice on protection for electronic communications networks; possible other requirements established in the Code, including information on possible legal action by right holders and reference to potential technical measures" ibid.
28. Ibid.
29. Ibid.
30. For more details ibid p. 41.
31. "The right to be identified with and to reasonably exploit one's own original creative endeavour" constitutes in his belief a human right. That it is completely within the legitimate standing of the company to act as an entity that which protects the law and Constitution and that "Internet is 'only' a means of communication and has not rewritten the laws of countries through which it passes."
32. Proyecto de Ley de Economía Sostenible http://www.economiasostenible.gob.es/wp-content/uploads/2010/03/01_proyecto_ley_economia_sostenible.pdf.
33. IFPI Digital Music Report 2010, "Music how, when, where you want it", avail. online http://www.ifpi.org/content/library/DMR2010.pdf.
34. We will refer to the most interesting part of the new Swedish Law –at least for our topic. The Court can order to an ISP to give the rights holder information on the identity of the user who is alleged to infringe copyright, under the condition that there is sufficient evidence. The principle of proportionality will apply while the interests of both parties (rights holder and alleged infringer) must be respected).
35. Regarding public awareness see Maria Canellopoulou-Bottis, "Public awareness of copyright issues: a perspective for the future". www.ccsr.cse.dmu.ac.uk/conferences/ethicomp/ethicomp2008/abstracts/ethicomp2008_bottis.php.
36. Isabel Davies & Stuart Helmer, E.I.P.R. 2008, 30(8), 307-308, Productores de Musica de Espana ("Promusicae") v Telefonica de Espana SAU ("Telefonica") (C-275/06).
37. Link: http://www.laquadrature.net/files/JURI_Gallo_report_adopted_EN.doc.
38. Thought 26, Gallo Report.
39. Thought 27, Gallo Report.
40. Thought 29, Gallo Report.

41. Thought 32, Gallo Report.
42. Franck Macrez & Julien Gossa «Surveillance et sécurisation: ce que HADOPI rate» RLDI -2009, N°50, 50-41 (§13). This article, that is quite critical to the HADOPI law, analyses why HADOPI will not have the results hoped by the government. The utility of HADOPI is exhausted before its coming into force since technology offers new possibilities to Internet users that cannot be detected easily. Besides, as mentioned by the authors of this article, the identification of the infringers is not such an easy task as expected.
43. Michel Vivant & Jean-Michel Bruguiere, Droit d'auteur, DALLOZ, First edition, 2009, p. 739.
44. On European level see Report Nantes mentioned above.

# The *sui generis* ontologies of the patent system

**Konstantinos Karachalios**

This is already the second time that I have the honour to be invited to speak at the Ionian University. Last year it was in the context of the Conference about Computer Ethical and Philosophical Enquiry, where we presented, together with the great Latin American thinker Laymert Garcia Dos Santos, different aspects of the contemporary battles around knowledge: geopolitical, technological, cultural and economical, in particular, how codified knowledge is generated, appropriated, controlled or shared [1].

The patent system is at the core of this big game. It became internationalised in 1883[2] and culminated a century later (in 1996) with the Trade Related Agreement on IP Rights, the so-called TRIPS, which introduced a detailed regulatory framework virtually all around the world, a singular success for an international normative undertaking[3]. In the same time, the corpus of patent-related, publicly available technical knowledge exploded to reach amounts and levels that are unprecedented in human history[4].

However, despite this success story, more and more people nowadays associate 'patent' with 'private', 'restricted', 'intransparent', 'unavailable'. This sounds much more like medieval times guild tradition than a post-renaissance state of mind. Moreover, it is an indictment for the *patent* system, the etymology of which derives from the Latin *patere* - which means to disclose, to lay open, to be clear - to be confused with *latent* (from Greek *λανθάνειν*), its exact antonym.

This tarnished reputation is the more surprising, as patent offices undertake very substantial efforts to make technical and legal information (e.g. legal status of patents) publicly available. They invest very significant resources in capturing, digitalising, classifying according to technical criteria, organising millions of documents every year in several collections[5] and putting this vast amount of technical information in public view, mostly free of charge. So where does this perception of intransparency come from?

## The transparency gap

Peter Drahos, a renown researcher of the patent system, expresses this societal unease and specifies it, when he says in a chapter titled "Taking transparency seriously" of his new book "The Global Governance of Knowledge"[6] that "...the

patent system currently does a very poor job of making information available to downstream inventors". He argues that "the obligation of patent offices is not just simply to publish the patent specification. This would be to construe the obligation passively. The purpose of the patent social contract is to diffuse invention information, simply to publish invention information in a patent office gazette is not the same as working towards actively spreading invention information. Turning patent offices from passive publishers into active diffusers of information requires patent offices to begin approaching their task much more like public libraries: finding creative ways to engage with very diverse user communities. The diffusion obligation of the patent office is not an obligation that is owed to a few wealthy corporate users of the patent system, but rather it is an obligation to society and to the many groups that are affected by monopolies over invention information. Patent offices obtain invention information from inventors by virtue of the operation of law. Under the social contract they should provide it as a public good. Moreover they should provide that information in ways that are useful to different user groups, ways that do not depend on patent searching expertise but rather more generalized skills of database searching. To date efforts in this direction have largely remained symbolic." Assuming that "... in theory it should be possible to have a technology platform that searched all the world's patents, allowing users to organize that information in various ways (around ownership, technologies, countries etc.)", he underlines the strategic and sensitive nature of this 'service', by claiming that "global patent transparency is the foundation upon which other reforms of the patent system have to be built." [7]

Whoever has tried to establish a comprehensive patent landscapes around HIV drugs or emerging environmental technologies, will have noticed how difficult is to get what you want. There are several reasons for this failure, in the following I will focus more on problems of a more structural nature. According to the present analysis, the fundamental problem is that this vast amount of information (several tens of millions of documents in the case of the EPO) is organised and structured in a way that it makes sense to the interior of the patent system, but not necessarily to its exterior. Why this?

## The role of classification schemes

Both libraries and patent offices use complex and sophisticated systems to classify and thus to store and retrieve information. According to Wikipedia: "A library classification is a system of coding and organizing library materials (books, serials, audiovisual materials, computer files, maps, manuscripts, realia) according to their subject and allocating a call number to that information resource. Similar to classification systems used in biology, bibliographic classification systems group entities together that are similar, typically arranged in a

hierarchical tree structure. A different kind of classification system, called a faceted classification system, is also widely used which allows the assignment of multiple classifications to an object, enabling the classifications to be ordered in multiple ways."

The same source states that "a patent classification is a way the examiners of patent offices or other people arrange documents, such as patent applications, disclosing inventions according to the technical features of the inventions. They arrange documents using a patent classification so that they can quickly find a document disclosing the invention identical or similar to the invention for which a patent is claimed. The same document may be classified in several classes." A patent classification system is a multi-faceted one.

## Patent Classification

Patent offices systematically classify patent documents as well as non-patent literature in order to assist with administration and patent searching. Patent classification systems are arranged in a hierarchical structure and provide different technologies with different alpha-numeric codes. This hierarchical structure is typically arranged into sections, subsections, classes, subclasses, groups and subgroups. Below is an example of how wind motors would be classified under the most commonly used classification system, the IPC.

Section F: Mechanical Engineering; Lighting; Heating; Weapons; Blasting

Subsections to Section F: Engines or pumps; engineering in general; lighting; heating; weapons; blasting.

Classes: E.g. F02: Combustion engines; F03 Wind, spring or weight motors.

Subclasses: E.g. F03D: Wind motors

Groups: FO3D 1/00: Wind motors with rotation axis substantially in wind direction.

Subgroups: F03D 1/02: With plurality of rotors

While the IPC system is the most widely used classification system, with approximately 70,000 subdivisions (covering documents published after 1968), it is not the most extensive. The European Classification system (ECLA) developed by the EPO builds on the IPC, includes up to 134,000 subdivisions and is made public via a multitude of databases, see e.g. the *esp@cenet* DB[8]. Internally, the EPO examiners also use further, much finer coding to organise the documentation in their field of expertise. Patent offices are thus, huge archiving and classification machineries, handling a vast amount of technical information daily, investing very significant resources to carry out this task. The classification and

re-classification exercise alone costs EPO some 140 FTEs[9] per year. In the framework of cooperation of the 5 major patent offices in the world (Patent offices of USA, Japan, China, Korea and the EPO) re-classification projects for harmonisation purposes is estimated to cost 2000 FTEs in the course of 10 years.

The quality of classification is absolutely crucial for the overall quality of the patent system. The exacter the classification, the better the search results and thus the comparison of the invention with the state of the art, and thus, the less trivial patents are granted.

## Comparing the two classification approaches

External similarities may sometimes conceal more than they reveal: although both systems follow a hierarchical tree structure, the rationale of how the tree branches are defined and grow are completely different. I assume, and please correct me if I am wrong, that librarians classify by grouping together entities that are similar, whereas the entities and the similarity should be defined in a way to make sense primarily to the users of the library and not to the librarians.

Unfortunately this is not always the case for existing patent classification systems. Patent examiners classify with the main purpose to help them carry out their own very specialised job. Patent classification is thus a priori an inwards looking process, the public perspective is not an important criterion. The result is that the complex ontologies[10] produced by the patent offices do not always make sense to the non-expert seeker of information. Although the existing publicly available patent information platforms and raw data collections[11] offer a significant potential service for skilled users, the system is often stretched to its limit. The service of delivering digital information to the public[12] entered the internet era with new technical tools, but without rethinking the basic concepts.

Let us try to use a metaphor. As we read above, libraries "group entities together that are similar", that means dogs are grouped together with wolves and crocodiles with other lizards. Patent offices group "according to the technical features" of an entity, that means they are rarely interested in the whole 'animal', they rather look at its specific use or fragment it into skin, nails, teeth, bones, meat etc. and group either according to this specific use or put these elements together with parts of other animals, the ingredients of which may be used for a similar purpose, whether the animals are similar to each other or not. Thus, the ontologies created by the patent system have very often nothing to do with lay-man's logic.

E.g., according to their utility, in Asia one would put dogs (more exactly, their flesh) in the food section, whereas in the West dogs would fall into the 'pet' category, together with canaries and cats. Similarly, crocodiles, because of their

leather, would be classified together with bovines, goats, snakes etc. and all together arranged probably in the section 'shoes' or by 'handbags, suitcases, etc'. Further, in African patent offices, because of their white meat, crocodiles would be classified also in the section of poultry.

Now, imagine someone trying to understand how a dog or a crocodile looks like by putting together, piece by piece, such a heterogeneous, fragmented documentation landscape. You must guess where you have to search for and you may still miss important information, e.g. that crocodiles have a vertebra and teeth, if you do not know that crocodile teeth or bones are used for buttons or something else of use to human kind.

## An example from the pharmaceuticals sector

You may think I am exaggerating and this is not a good example. Then, take instead of 'dog', 'Tamiflu' or '*oseltamivir*' and carry out a keyword search with *esp@cenet*: you would find some 72 patents classified in a variety of groups. I bet with you that the number of patents related to this drug and its variations is orders of magnitude bigger than this. To get them all one needs either a very high expertise or a lot of money for specialised patent information providers.

An example why this is an important issue: some years ago, the World Health Organisation tried to establish a list showing whether some essential drugs were patent protected in a given set of developing countries or not. They believed that the lack of this very basic information was hindering national and international procurement agencies and NGOs from buying and importing cheap generic drugs in these countries. Dealing with this problem has become an important aspect of the Global Strategy and Plan of Action on Public Health, Innovation and Intellectual Property of the World Health Organisation.

The EPO became involved in this project, and unsurprisingly, what soon became clear was that this was no simple task. Many patent offices in the target countries were not able to deliver a clear answer to what seems to be a simple question, namely: "Is the patent application with publication/priority number X that was filed in your country on date Y still in force?". It is hard to believe that a patent office is unable to deliver this information, which theoretically, should be simple. The main source of failure was the lack of adequate documentation systems, resulting in situations like this: "Swiss drug major Roche has told the governments of Indonesia, the Philippines and Thailand that they are free to manufacture generic versions of its anti-influenza drug Tamiflu (oseltamivir) because it is not patented in their countries. Roche says it received "with surprise" the announcement that Taiwan planned to issue a compulsory license for Tamiflu ..."[13]. Several years on, it is clear that there does not appear to be any easy way to resolve

this complex tangled web, particularly with many small patent offices under-resourced, as transparency costs money.

## The carbon capture example

You may say, drugs is a complex case, in engineering logic dogs would be with wolves, and crocodiles with lizards. Really? Let's take instead of 'crocodile' the case of the important emerging technology characterised as CO2 capture, sequestration and storage (CO2 CSS). It means that CO2 is taken out of combustion gases and stored in the earth, instead of being released into the atmosphere.

Trying to get a complete list of patented technologies in this field via IPC is no mean feat. It is like looking for an unknown number of needles of unknown size in 8 different hay stacks. Caution: in the patent game you win only if you have found all needles. First, you have to decide in which of the eight IPC sections (hey stacks) you should look for:

| | **The eight main IPC and ECLA sections** |
|---|---|
| A | Human necessities |
| B | Performing operations; transporting |
| C | Chemistry; metallurgy |
| D | Textiles; paper |
| E | Fixed constructions |
| F | Mechanical engineering; lighting; heating; weapons; blasting engines or pumps |
| G | Physics |
| H | Electricity |

To cut a very long story short, technologies to capture and store CO2 are categorised in no less than four of these sections (B, C, E and F), and within each section in most cases in many 'branches' that are far from each other. The patent offices are therefore since February 2010 suggesting a list of categories as a first start (a so-called 'catchword index' service). So, if one enters the search words "carbon capture" in the classification search mask of *esp@cenet,* following 'help' is offered to the desperate information seeker

| | |
|---|---|
| • Separation of gases or vapours; Recovering vapours of volatile solvents from gases; Chemical or biological purification of waste gases, e.g. engine exhaust gases, smoke, fumes, flue gases, aero.... | B01D53 ☐ |
| • Arrangement of devices for treating smoke or fumes (treating smoke or fumes, see the relevant class for the treatment, e.g. B01D53/00) | F23J15 ☐ |
| • Supplying non-combustible liquids or gases, other than air, to the fire, e.g. oxygen, steam | F23L7 ☐ |

| | |
|---|---|
| • Separating dispersed particles from gases, air or vapours by liquid as separating agent (B01D45/10 takes precedence; fractionating colum.... | B01D47 ☐ |
| • Hydrogen; Gaseous mixtures containing hydrogen; Separation of hydrogen from mixtures containing it (separation of gases by physical means B01D);.... | C01B3 ☐ |
| • Equipment or details not covered by groups E21B15/00 to E21B40/00 | E21B41 ☐ |
| • Compounds of calcium, strontium, or barium (C01F7/00 takes precedence) | C01F11 ☐ |
| • Electrolytic production of inorganic compounds or non-metals | C25B1 ☐ |
| • Carbonates of sodium, potassium or alkali metals in general | C01D7 ☐ |
| • Carbon; Compounds there of ([N: C01B6/00], C01B21/00, .... | C01B31 ☐ |

I am not sure how encouraging this looks even to hard core experts. Moreover, since most categories do not deal specifically with CO2, but generally with gases and fluids, even if you wander through all these labyrinths and retrieve the related documents, you would still have to filter-out CO2 from all other gases and liquids, and - believe me - this is less than evident a procedure.

One of the best experts in the field, consulting US venture capitalists for investments in the carbon capture domain, told me[14] that it took him 8 months of iterative work through the hay stacks to find 6000 of them. He apparently still missed one third (EPO identified some 9000 patents related to CO2 CSS).

In my humble opinion, this cannot be seen as a serious attempt to help information seekers in such critical fields. But there are other, politically far more critical consequences from this failure.

## UNFCCC negotiations around technology transfer and the role of patents

The incapacity of the patent system to deliver timely and meaningful sector-related information around technologies with a potential of reducing greenhouse gas emissions creates growing political tensions in the climate change debate. Radical proposals are being tabled and experts attending the UN conference maintain that patents have become the most polarised and controversial item on the agenda. In fact this is the only field where no progress has been achieved. On the contrary, as the battle lines are drawn up, there seem to be no zones of compromise between the growing number of black or white positions being taken. Governments, their negotiators, researchers, political analysts, industry and other stakeholders are expressing an urgent need for platforms to provide continuous and reliable, sector- and country-related information about relevant technologies, their ownership and the costs associated with their acquisition.

That things do not need to be like this, shows an example from a recent engagement by the EPO. The EPO first identified potential risks to the IP system posed by fallout from the climate change debate in 2006, during work on the above mentioned "Scenarios for the Future" study, which was a long time before IP was seen elsewhere as even a mild indicator of trouble on the horizon. However, it soon became apparent that the issue was too complex for a single institution to handle on its own and that broader alliances would be necessary with organisations which have access to complementary expertise.

In 2009, a formal agreement was reached on a programme of co-operation between the EPO, the UN Environment Programme (UNEP) and the International Centre for Trade and Sustainable Development (ICTSD), a leading NGO specialising in sustainable trade and technology transfer. The aim of this programme was to launch an empirical study to shed light on the role of patents in the transfer of climate change mitigation technologies. More partners soon joined in: the OECD Environment Directorate, leading business and industry associations (such as the International Chamber of Commerce (ICC), the Licensing Executives Society International (LESI), the World Business Council for Sustainable Development, and the Fraunhofer Gesellschaft), specialised governmental agencies like the Energy Research Centre of the Netherlands, and other NGOs and intergovernmental organisations. It was a first step towards creating a unique alliance among very diverse partners. In parallel the EPO acquired observer status at the UN climate change conference.

Carrying out the study, technologies in the field of renewable energy, biofuels and so-called "clean coal" were mapped first. On the basis of this work, the EPO and external experts developed a new taxonomy of technologies and their applications, down to apparatuses and components. Patent examiners performed searches and retrieved worldwide patent data relating to these categories. Using this data, the OECD then carried out various statistical analyses, looking at development trends over time in specific sectors and countries. In this way, precise patent landscapes were established for the technologies under scrutiny. In parallel, a first-ever licensing survey was carried out among technology developers and potential licensors in the field of environmental technologies[15].

One and a half years later, all project targets have been met and the final report is expected to be published in the autumn of this year. The study not only provides many politically and otherwise relevant findings, it also makes suggestions for further analysis and research in the field. However, it shares the same fate as all other analyses on the same or similar topics - it only constitutes a snapshot in a vast, dark space. We came to realise this, but also noted that the collection of patent data itself would constitute a very valuable asset for experts and other special

interest groups alike. To match this need, the EPO decided to take advantage of the effort already invested and use it to produce a publicly available, continuous flow of patent information relating to the energy sector. A genuine new public good would thus be created for the benefit of the global knowledge economy.

The ideal solution proved to be a new, detailed classification scheme similar to others previously developed by the EPO to track and categorise new technological developments, such as nanotechnology. The scheme is designed to serve as an interface between the vast amount of technical knowledge contained in the patent documentation, and the information needs of society. To achieve this, the entire worldwide patent documentation had to be re-classified into more than 200 new categories[16].

Apart from being easily accessible to and understandable by non-experts, this new information tool will always be kept up to date and accurate. Embedding it in the EPO's classification scheme ensures that the collective intelligence of 4000 patent examiners and classification experts maintains and improves it automatically on a daily basis. A better solution could hardly have been found.[17]

The Y02 subclasses already available to the public relate to clean energy technologies, namely Y02C (greenhouse gases- capture and storage/ sequestration or disposal) and Y02E (greenhouse gases - emissions reduction technologies related to energy generation, transmission or distribution). The new ontology for the 'animal' carbon capture and storage looks now like this[18]:

| SECTION Y - GENERAL TAGGING OF NEW TECHNOLOGICAL DEVELOPMENTS | |
|---|---|
| ECLA Code | Description |
| Y02: | TECHNOLOGIES OR APPLICATIONS FOR MITIGATION OR ADAPTATION AGAINST CLIMATE CHANGE |
| Y02C: | Capture, storage, sequestration or disposal of greenhouse gases (GHG) |
| Y02C10/00: | CO2 capture or storage |
| Y02C10/02: | Capture by biological separation |
| Y02C10/04: | Capture by chemical separation |
| Y02C10/06: | Capture by absorption |
| Y02C10/08: | Capture by adsorption |
| Y02C10/10: | Capture by membranes or diffusion |
| Y02C10/12: | Capture by rectification or condensation |
| Y02C10/14: | Subterranean or submarine CO2 storage |

Thus, search work that required significant expertise, time and money can now be done by any interested person who knows that the system exists and what he/ she is looking for. Of course,, there is another dimension, beyond technical de-

tails: in the era of the knowledge economy, making codified and pertinent information accessible to broader constituencies amounts to a genuine political act. It reduces the power and control of incumbent experts for the benefit of society.

You may go and convince yourself how easy is to retrieve what you want, by simply copying the code into the search mask[19]. Instead of erring into the labyrinthic galleries of the patent classification, you have an 'one stop-shop'. With one 'click' on the right side box one can copy this code into the *esp@cenet* search mask and would thus get all patents worldwide related to these technologies and only these. By adding a second criterion in the search mask (e.g. country code in third line) one can get all patents in a given technology field for a certain country. One could add also a company name, getting only patents submitted by this company, etc...

The Y02E subclass, for example, looks like this:

| Code Y02E | Description | Comment |
|---|---|---|
| 10/00 | Energy generation through renewable energy sources | Geothermal, hydro, oceanic, solar (PV and thermal), wind |
| 20/00 | Combustion technologies with mitigation potential | CHP, CCPP, IGCC, synair, cold flame, etc. |
| 30/00 | Energy generation of nuclear origin | Fusion and fission |
| 40/00 | Technologies for efficient electrical power generation, transmission or distribution | Reactive power compensation, efficient operation of power networks, etc. |
| 50/00 | Technologies for the production of fuel of non-fossil origin | Biofuels, from waste |
| 60/00 | Technologies with potential or indirect contribution to GHG emissions mitigation | Energy storage (batteries, ultracapacitors, flywheels...), hydrogen technology, fuel cells, etc. |
| 70/00 | Other energy conversion or management systems reducing GHG emissions | Synergies among renewable energies, fuel cells and energy storage |

And here is the breakdown for a particular group (solar energy):

| Code Y02E | Description |
|---|---|
| 10/40 | Solar thermal energy |
| 10/41 | Tower concentrators |
| 10/42 | Dish collectors |
| 10/43 | Fresnel lenses |
| 10/44 | Heat exchange systems |
| 10/45 | Trough concentrators |
| 10/46 | Solar-thermal plants for electricity generation, e.g. Rankine, Stirling solar-thermal generators |
| 10/47 | Mountings or tracking |

| | |
|---|---|
| 10/48 | Mechanical power, e.g. thermal updraft |
| 10/50 | Photovoltaic (PV) energy |
| 10/52 | PV systems with concentrators |
| 10/54 | Material technologies |
| 10/54B | CuInSe2 material PV cells |
| 10/54D | Dye sensitized solar cells |
| 10/54F | Solar cells from Group II-VI materials |
| 10/54H | Solar cells from Group III-V materials |
| 10/54J | Microcrystalline silicon PV cells |
| 10/54L | Polycrystalline silicon PV cells |
| 10/54N | Amorphous silicon PV cells |
| 10/56 | Power conversion electrical/electronic aspects |
| 10/56B | for grid-connected applications |
| 10/56D | concerning power management inside the plant, e.g. battery charging/ discharging, economical operation, hybridisation with other energy sources |
| 10/58 | M.P.P.T. systems (maximum power point tracking) |
| 10/60 | TPV hybrids |

This scheme was publicly released on 9 June 2010 at a side event of the 32nd Subsidiary Bodies meeting of the UNFCCC in Bonn. The question of accessibility to and costs of such privately owned technologies is a matter of permanent friction for the ongoing (rather not ongoing) negotiations. The new scheme is meant as an offer to negotiating parties who explicitly express following need:

"A technology information platform should be developed and be continuously updated to collect information on sector-specific technologies and best practices on publicly and privately held technologies, including on IPRs and licensing, costs, abatement potentials, and manufacturers of technologies."[20]

We are therefore confident that this work has the potential to accommodate a big part of the above mentioned claims of the UNFCCC for a continuous, transparent and reliable technology information platform**.** However, whether further technology sectors (buildings, transportation, industry, agriculture, waste management) could be dealt with as a follow-up of this project is still an open question. In particular, since the definition of the new categories is the most critical and politically sensitive point (to which questions should the new categories deliver answers and who is posing them?), it would be important to collaborate with experts from key developing countries and/or with the UNFCCC secretariat to co-shape the remaining sectors. The EPO may even apply this methodology to create similar ontologies for other politically critical technical fields (essential drugs, ICT standards). Finally, the process can be further improved, in particular by making the classification rules explicit and public[21].

Concluding, the platform created by the EPO offers to non-expert seekers of patent-related information in the clean energy field following services:

- Worldwide patent coverage (not only EP, US etc. patents).
- All relevant technologies gathered together in one place, i.e., no in-depth knowledge of IPC or ECLA necessary.
- Detailed break-down up to component level (for example: dye-sensitized solar cells, off-shore wind towers, IGCC, torrefaction of biomass, direct methanol fuel cells, smart grids etc. all have their own separate entries).
- Regularly updated with the newest patent publications.

For now, however, this successful effort is further evidence that the patent system has the potential to rise to the expectations according to the original meaning of its name by providing comprehensive, useful information to the public, starting from a very critical, strategically important field[22].

## Endnotes

1. See: Scenarios for the Future, EPO, 2007.
2. The Paris Convention for the Protection of Industrial Property, signed in Paris in 1883, was one of the first intellectual property treaties. As a result of this treaty, intellectual property, including patents, of any contracting state are accessible to the nationals of other states party to the Convention.
3. Peter Drahos, and John Braithwaite, Information Feudalism: who owns the knowledge economy?; Earthscan, 2002.
4. Alone the EPO patent databases include some 60 million documents. See also Spinello R. & Bottis M., A defense of intellectual property rights, 2009. For a history of patents in Greek, see Bottis M., Information law, 2004.
5. See EPO's numerous subscription DBs in http://www.epo.org/patents/patent-information/subscription.html.
6. Peter Drahos, The Global Governance of Knowledge, Cambridge University Press, 2010 (Chapter 11: Reclaiming the patent social contract - Taking transparency seriously).
7. See also argumentation by Konstantinos Karachalios and Shirin Elahi in: Transparency, Trust, and the Patent System, Journal of Intellectual Property Law & Practice, Sept. 2009.
8. http://www.espacenet.com/index.en.htm.
9. FTE: full time employee, in EPO's case this is a fully trained examiner, our most precious asset
10. According to Wikipedia: In computer science and information science, an ontology is a formal representation of the knowledge by a set of concepts within a domain and the relationships between those concepts. It is used to reason about the properties of that domain, and may be used to describe the domain. In theory, an ontology is a "formal, explicit specification of a shared conceptualisation". An ontology provides a shared vocabulary, which can be used to model a domain - that is, the type of objects and/or concepts that exist, and their properties and relations. Ontologies are used in artificial intelligence, the

Semantic Web, systems engineering, software engineering, biomedical informatics, library science, enterprise bookmarking, and information architecture as a form of knowledge representation about the world or some part of it.

11. For an overview of the free of charge information services of the EPO, see http://www.epo.org/patents/patent-information.html.
12. An example of how one can use classification systems to retrieve information is presented in EPO's *esp@cenet* assistant 'How do I use the Classification search?' http://v3.espacenet.com/eclasrch?classification=ecla&locale=en_EP.
13. 'Tamiflu compulsory license not necessary, Roche tells three Asian nations', Pharma Marketletter, 5-12-2005.
14. Communication during a teleconference in January 2010.
15. About the project, see http://www.epo.org/topics/issues/clean-energy.html.
16. Look into Class Y02 in http://v3.espacenet.com/eclasrch?classification=ecla&locale=en_EP&ECLA=y02.
17. For more explanations about this new classification scheme, see http://www.epo.org/topics/issues/clean-energy/classification.html, in particular the white paper http://documents.epo.org/projects/babylon/eponet.nsf/0/6e41c0df0d85c0acc125773b005144de/$FILE/clean_energy_brochure_en.pdf.
18. See http://ep.espacenet.com/advancedSearch?EC=Y02C10/04 for searching carbon capture by chemical means.
19. http://v3.espacenet.com/eclasrch?classification=ecla&locale=en_EP&ECLA=y02c10.
20. See e.g. Paragraph 194, page 150 of UNFCCC FCCC/AWGLCA/2009/8.
21. E.g. via hypertext language; see Building a Companion Website in the Semantic Web. Timothy Miles-Board et al.; Proceedings of the 13th international conference on World Wide Web 2004; http://www.iw3c2.org/WWW2004/docs/1p365.pdf.
22. For an example of the resonance, see http://cleanip.com.au/2010/06/18/at-last-clasification-system-for-climate-change-technologies/.

# Information technology, democratic societies and competitive markets

**Iordanis Kavathatzopoulos**

## Introduction

Democracy and free markets are today at the focus of debate and politics. A lot of discussions but also polemics are about these issues, nationally and internationally. It seems sometimes that the main reason behind conflicts and even wars are lack of democracy and market freedom. Still we have to raise the question if this is important: If democracy and functioning markets are important for the well being of societies and people.

Starting from the issue of high living standards and supply of necessities for our lives we can see that the main argument may be that democracy and market economy can provide us with what we need. But let us make a thought experiment and for the argument's sake suppose that another political system, for example en enlightened and tolerant oligarchy, could provide us with most of the things we need to have a good life. Would this or any other political system providing these thing, be a good system? Is it something that we could accept?

No, we do not accept this. There is a significant difference between an authoritarian and a democratic political system, at least in theory. An authoritarian system may provide most of the material, and probably immaterial things people need but this is done by the rulers, not by the people. This means that the rulers do what they want. Of course, whenever they like, they can change their mind. In such a system people cannot control any supply of any necessity.

Power is the crucial thing here. People need and want to have the power to rule their own lives. Here we can point to the problem of knowing the real needs of the people, which is another important factor. It would be very difficult, even for the most benevolent ruler to know what the needs of the people are. People themselves know this. Still, the main reason for being skeptical to good non-democratic systems, if there are any, is that what is delivered is something that it is not decided by people themselves but by rulers who may be good today but maybe not tomorrow.

So democracy is a social process of negotiating solutions, like in a free market, where all stakeholders participate. How this is done and what decisions are made

depends on the participants. There are two issues that are of importance here. First, there is the issue of the basic characteristics of democracy and of free market, and the conditions that make these social processes possible. Second, there is the issue about the certain skills participants must have to be able to uphold a democratic political process or a free market negotiation process.

## Democracy and free market

There are many interpretations of the words democracy and free market. How democratic a society is or how free and competitive a market is cannot be defined only by things like high living standards, good economy, social security, daycare, schooling, and protected environment. Democracy and free competitive market are the way such things are decided. Still people have a formalistic approach to this issue. The most common view is that democratic processes, institutions and formal procedures define democracy. However, one may ask the question if it could be possible to run democratic institutions and processes undemocratically, for example letting a few people make all important decisions in dark rooms and then use the democratic processes as a show. Indeed there are powerful groups with strong interests in our society and in the markets as well as an indifferent majority of citizens and consumers allowing for example lobbying to be very significant in decision making.

Focus on power relations has always been the dominating approach to the definition of democracy and free market. The power of strong groups or persons hindering democracy and free trade, imposing tyranny, oligarchy, dictatorship, crippled democracy and the like has been on the main focus of the effort to understand undemocratic systems as well as to act against them and to support democracy (Dahl, 1989). No one should ignore this but let us consider another factor or dimension that might be at least of equal importance, namely the will of people to participate in the political or market negotiation processes and their ability to run these democratically or competitively. We can easily understand that if people do not want to search solutions to their problems in a dialog together with others or if they cannot do it properly democracy or free market are not there (Hayek, 1944; Popper, 1945). It is therefore important to try to understand the psychological conditions under which dialog and negotiation are possible and base our efforts to promote democracy and competitive markets on this understanding.

It is impossible to make a general and longitudinal plan for products and services that people demand. The reason for that is that the demand always changes. Therefore the only possible way to satisfy demands for products and services is creating a free and competitive market. A market like that is flexible enough to

adjust to the needs whenever they appear or change. In that sense problems have to be solved and decisions have to be made constantly by consumers and producers about what and how to produce or to purchase. In this process judgments have to be made about the offers in relation to needs. Contracts and agreements have to be made. This is the process of negotiation.

For this negotiation process to succeed balance between partners is a condition as well as objective information about the product or service at hand. It has been already pointed out, with many examples from history, that without freedom and equality between partners it is impossible to achieve fulfillment of the goals of all partners. Formally equality in market relations is there in most countries of the world. However, objective information is necessary for the negotiation process to be balanced. Objective information is a condition for a negotiating part to analyze, compare and weigh the facts to make the right decision. For each part it is important to analyze critically and self-critically the situation for himself, i.e. have an internal negotiation about own needs related to what is on offer (Fig. 1). If the picture provided by the information is false then the internal analysis will be biased as well as the following negotiation with the other part.

In the political process democracy is similar to negotiation in markets. In essence democracy is dialog between people. That means that people search for solutions to their problems by thinking together with others. But that presupposes that each person has a dialog with himself and that each person starts with the position that own ideas and beliefs need to be better. This makes it possible to listen to others. Each participant in a democratic process, or a dialog, feels always the need of other participants because he is expecting them to help him to find a better idea than the one he holds for the moment. If one trusts own beliefs and does not question own knowledge there is no reason to search for something better. Thereby dialog and democracy become impossible (Fig. 1).

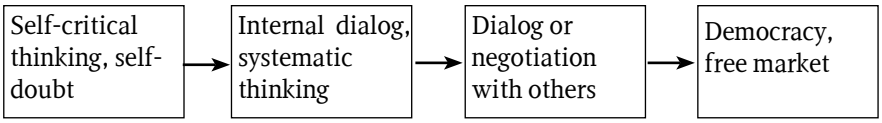



*Figure 1*. Skills for democracy and free market.

This is true about persons, but it is also valid on a societal level. Absolute truths in a society or in a market, for example taboos or political correctness, established brands, do not allow critical thinking, dialog and democracy just because there is nothing better to search for. On the contrary every effort for dialog or objective information can be understood as a provocation that nobody wants to listen to, or worse it can be seen as a criminal act, e.g. defamation, offence, leading to suppression and punishment.

Anyway the democratic problem in our industrialized and global society is not the brutal use of force to suppress free thinking and dialog, missing democratic institutions and procedures, or forbidden free negotiations and the hand out of special privileges to certain market players. Rather the problem lies with running and upholding a dialog that makes a democratic sense, in the way persons think and in the way individual citizens and groups communicate, negotiate and cooperate. There are many factors affecting this but is there anything that can contribute to a better ability for dialog and negotiation?

## Skills for dialog and negotiation

Usually we think that what we can do is to transmit values and principles, for example equality, respect for individual rights, etc. But do we need that? Are people undemocratic because they lack certain principles? This is of course not true. Certain principles and values are necessary to participate fruitfully in a dialog. People usually have these principles; the problem may be how to apply them. The other problem is what principles should be valid. Is it possible for everybody involved to agree on that? Is it possible to achieve agreement on what are the right democratic principles among different interest groups or among philosophers and political scientists?

In educational programs we can teach the structure and processes of democracy and dialog. We can train people to participate in a meeting, to know how to make propositions, motions, how to act as chairman, how to vote and how to count votes. But although this is necessary and facilitates dialog it is only a frame, or a tool. Without a substance it has no value. It cannot by itself trigger dialog and democracy.

Starting from one of the most important contributions, the Socratic dialog, we see that *aporia* is the goal rather than the achievement of a solution to the problem investigated. Reaching a state of no knowledge, that is, throwing aside false ideas, opens up for the right solution. The issue here for the philosopher is not to provide a ready answer but to help the other person in the dialog to think in the right way (Πλάτων [Platon], 1981, 1992b). Ability to think in the right way is not easy and apparently has been supposed to be the privilege of the few able ones (Πλάτων [Platon], 1992a). For that, certain skills are necessary, such as Aristoteles's *fronesis* ('Αριστοτέλης [Aristoteles], 1975). When humans are free from false illusions and have the necessary skills they can use the right method to find the right solution to their moral problems (Kant, 1785/2006).

This philosophical position has been applied in psychological research on ethical decision making. Focusing on the process of ethical decision making psychological research has shown that people use different ways to handle problems.

According to Piaget (1932) and Kohlberg (1985), when people are confronted with moral problems they think in a way which can be described as a position on the heteronomy-autonomy dimension. *Heteronomous* thinking is automatic, emotional and uncontrolled thinking or simple reflexes that are fixed dogmatically on general principles. Thoughts and beliefs coming to mind are never doubted. There is no effort to create a holistic picture of all relevant and conflicting values in the problem they are confronted with. Awareness of own personal responsibility for the way one is thinking or for the consequences of the decision are missing. *Autonomous* thinking, on the other hand, focuses on the actual problem situation, and its main effort is to search for all relevant aspects of the problem. When one is thinking autonomously the focus is on the consideration and investigation of all stakeholders' feelings, duties and interests, as well as all possible alternative ways of action. In that sense autonomy is a systematic, holistic and self-critical way of handling a problem.

Handling problems autonomously means that a decision maker is unconstrained by fixations, authorities, uncontrolled or automatic thoughts and reactions. It is the ability to start the thought process of considering and analyzing critically and systematically all relevant values in a problem situation. This may sound trivial, since everybody would agree that it is exactly what one is expected to do in confronting a problem. But it is not so easy to use the autonomous skill in real situations. Psychological research has shown that plenty of time and certain conditions are demanded before people can acquire and use the ability of autonomy (Sunstein, 2005).

Focus should then be on supporting autonomy, i.e. self-critical and systematic thinking. That would be targeting the real aim, since self-criticism and self-doubt are the main preconditions for dialog and negotiation. Furthermore, self-criticism, dialog and systematic searching seem to be the way democratic principles, institutions and procedures as well as free and competitive markets, are created and maintained.

This is not easy to achieve, and it may be hindered by some kind of framing, or by irrelevant and false information. Nevertheless, there are people who have learnt to use autonomy more often, usually people at higher organizational levels or people with higher responsibility (Kavathatzopoulos & Rigas, 1998, 2006). Training and special tools do also support the acquisition of the skill of autonomy. Research has shown that it is possible to promote autonomy. It is possible through training to acquire and use this skill longitudinally and in real life (Kavathatzopoulos, 1993, 1994, 2004).

Indeed new technology has certain features that can contribute to strengthening democracy in many of its aspects. For example one important condition for

democracy is information to citizens. New technology can make it much easier to inform people about all kind of issues as well as to provide a lot of services at a very low cost and much more effectively. But although this is important and something that citizens appreciate highly it is not what democracy is about. Rather it can be criticized as treating people more as passive consumers than active citizens.

Although equality and other formal institutions and regulations are very important for democracy, information has a special weight both for political dialog and for negotiation in the market (Hayek, 1944). Information has to be accurate and accessible whenever needed. It is obvious that Information Technology can contribute a lot here.

But this is not enough. Information has also to be of such a kind that it can support autonomy, i.e. rational thinking, during the negotiation process. Sadly the case is rather the opposite: Information about products and services is usually formed, structured and presented in a way to confuse the critical, self-critical and systematic thinking of the receiver. Commercials, placing of products in supermarkets, pricing (e.g. 199 instead of 200), etc. are some telling examples of how this is working. There are some markets though, like stock markets, where this is absolutely forbidden. There are strict regulations on what, how and when information is presented, with the explicit aim to support receiver's independent and critical thinking.

Information Technology can contribute a lot here by providing necessary information. With almost no cost consumers can get information about the quality of products as well as about competitive issues such as prices, stock, etc. Furthermore, properly constructed IT systems can be used to stimulate autonomy during a process of problem solving and decision making, for example EthXpert (Kavathatzopoulos & Laaksoharju, 2010; Laaksoharju & Kavathatzopoulos, 2009)

## IT supporting skills

New technology can make information from authorities and political institutions that citizens themselves feel is important more accessible and therefore facilitate citizens participation in political decision making. New technology can support openness and by that invite people to be more aware and active. Furthermore, it can support horizontal communication among citizens and consumers. Issues that are of interest to few people or to people that for some reason have difficulties to contact each other by traditional means may be neglected in the political process, or be marginalized in markets, even though they are important. IT systems can easily overcome such difficulties and provide a powerful tool to connect, inform and coordinate people's actions in market and in politics.

But Information Technology comes with some risks. One such risk is making it much easier to gather all kind of information about citizens or consumers, and therefore hurt their integrity. Actually, spying on people leads inevitably to less powerful citizens, to less democratic political systems, and to biased markets. Another risk is isolating oneself, alone or in groups with other likeminded people, making it much more difficult to affect other groups and to participate in other political or market processes that might be important for one's primary interests.

New technology can contribute to self-critical and systematic thinking, which is the base for successful dialog and negotiation. Indeed IT systems have many advantages that can be used for the promotion of democratic and market skills. Information Technology saves time and space, it has an enormous memory storage capacity, it can process and reorganize information fast and reliably, etc. Recent technical developments in particular, which give us the possibility to construct advanced games and simulate the complexity of reality in micro worlds, may further broaden the spectrum of opportunities and possibilities for support in dialog and negotiation (Laaksoharju & Kavathatzopoulos, 2008).

## Necessary policies and risks

Information Technology tools can stimulate self-criticism and systematic internal dialog. However, in searching to promote democratic and market skills we need to be assured that self-critical and systematic thinking is indeed stimulated by the support tools we use. Training and support of skills are educational issues, but also dependent on policies and laws. For such education to take place and have the expected effect it must be allowed, accepted and supported by society. Running a process like that, using training programs and tools for rational thinking successfully, is dependent on a framework that allows and supports it. The issue is if that can really happen.

Correct and relevant information can be provided much easier by the use of IT tools, for example about political issues, quality of products, prices, etc. However, the main belief in society is that information must be "free" in the sense of freedom of speech, meaning that the provider of information may formulate the message as he wishes. The result of this is that the strong actors in politics as well as in markets control the content and the form of information, according to their interests. That is why this is not allowed in stock market; all actors there are strong and very well aware of the importance of rational thinking.

Rules and laws are needed to guarantee the qualities of information necessary for the stimulation of rational mental processes in dialog and negotiation. But is this possible? Could it be good for society? Could it perhaps create anxiety and anarchy instead of democracy and competitive markets?

Of course we expect strong actors in politics and in markets to react negatively and oppose all measures taken in that direction. They will certainly do the best they can to stop such developments, but a legal framework pushing toward critical thinking may also cause anxiety and insecurity on the part of most citizens and consumers since they will be aware or their own power and responsibility. Would they be ready to accept that? Our current political and market systems are undoubtedly biased, but still functioning. More or less they provide us with what we think we need, at least in the so-called developed world. Is it possible for us to accept the risk of creating problems or, more seriously, paralyzing the whole system because we want to make it better?

## References

'Αριστοτέλης [Aristoteles]. (1975). 'Ηθικά Νικομάχεια [Nicomachean Ethics]. Πάπυρος [Papyros]: Αθήνα [Athens].

Dahl, R. (1989). Democracy and its critics. Yale University Press: New Haven.

Hayek, F. (1944). The road to serfdom. London: Routledge.

Kant, I. (1785/2006). Grundläggning av sedernas metafysik [Grundlegung zur Metaphysik der Sitten/Groundwork of the metaphysics of morals]. Daidalos, Stockholm.

Kavathatzopoulos, I. (1993). Development of a cognitive skill in solving business ethics problems: The effect of instruction. Journal of Business Ethics, 12, 379-386.

Kavathatzopoulos, I. (1994). Training professional managers in decision-making about real life business ethics problems: The acquisition of the autonomous problem-solving skill. Journal of Business Ethics, 13, 379-386.

Kavathatzopoulos, I. (2004). Making ethical decisions in professional life. In H. Montgomery, R. Lipshitz and B. Brehmer (Eds.), How professionals make decisions (pp. 277-288). Lawrence Erlbaum Associates Inc.: Mahwah, NJ.

Kavathatzopoulos, I. and Laaksoharju, M. (2010). Computer aided ethical systems design. In M. Arias-Oliva et al. (Eds.), The "backwards, forwards, and sideways" changes of ICT (332-340). Universitat Rovira i Virgili: Tarragona, Spain.

Kavathatzopoulos, I. and Rigas, G. (1998). A Piagetian scale for the measurement of ethical competence in politics. Educational and Psychological Measurement, 58, 791-803.

Kavathatzopoulos, I. and Rigas, G. (2006). A measurement model for ethical competence in business. Journal of Business Ethics Education, 3, 55-74.

Kavathatzopoulos, I. (2003). The use of information and communication technology in the training for ethical competence in business. Journal of Business Ethics, 48, 43-51.

Kavathatzopoulos, I. (2005). Computers for ethical competence. In G. Collste, S. O. Hansson, S. Rogerson, and T. W. Bynum (Eds), ETHICOMP 2005: Looking back to the future [CD-ROM]. Linköping University: Linköping.

Kohlberg. L. (1985). The Just Community: Approach to moral education in theory and practice. In M. Berkowitz and F. Oser (Eds.), Moral Education: Theory and application. Lawrence Erlbaum Associates: Hillsdale, NJ.

Laaksoharju, M. and Kavathatzopoulos, I. (2008). Can micro world simulations assess and stimulate ethical competence? In T. W. Bynum, & R. Simon (Eds.), Living, working and learning beyond technology (pp. 503-510). Mantova, Italy: Univeristy of Pavia.

Laaksoharju, M. and Kavathatzopoulos, I. (2009). Computerized support for ethical analysis. In M. Botti et al. (Eds.), Proceedings of CEPE 2009 – Eighth International Computer Ethics and Philosophical Enquiry Conference. Ionian University: Kerkyra, Greece.

Piaget, J. (1932). The moral judgement of the child. Routledge and Kegan Paul: London.

Πλάτων [Platon]. (1981). Θεαίτητος [Theaitetos]. Ι.Ζαχαρόπουλος [I. Zacharopoulos]: Αθήνα [Athens].

Πλάτων [Platon]. ( 1992a). Πολιτεία [The Republic]. Κάκτος [Kaktos]: Αθήνα [Athens].

Πλάτων [Platon]. (1992b). 'Απολογία Σωκράτους [Apology of Socrates]. Κάκτος [Kaktos]: Αθήνα [Athens].

Popper, K. R. (1945). The open society and its enemies. Routledge and Kegan Paul: London.

Sunstein, C. R. (2005). Moral heuristics. Behavioral and Brain Sciences, 28, 531-573.

# Regulating speech on the Internet: myths, trends and realities

**Panagiota Kelali**

## Introduction

In the early days of its existence, the "international network of interconnected computers"[1] was hailed as the "information superhighway"[2] and was viewed by many as the ultimate means to expand the freedom of speech worldwide.[3] As the court in *ACLU v. Reno*[4] explained, "it is no exaggeration to conclude that the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country - and indeed the world - has yet seen."[5] Indeed, users could become their own editors, disseminate information and give their opinions on a global scale. Free expression, distribution and reception of information never seemed so complete. For more than a decade, the Internet has been conceptualized as a forum for free expression with near limitless potential for individuals to express themselves and to access the expression of others holding the promise of an open platform for the exchange of ideas, accessibility, ease for mastery, and creativity. Internet was hailed as a place that knew no boundaries, where no sovereign ever reigned where anonymity and freedom of expression seemed to be safely guarded. However, reality turned out to be slightly different. The current proliferation of global information networks has prompted governments to regulate communication on these systems.[6]

As of December 31, 2009, Internet users were 1, 802, 330, 457, an increase of 399% since 2000.[7] Undoubtedly the Internet has evolved to become the premier avenue of communication in the 21st century. There is no other medium where the single act of sharing information can raise issues of freedom of expression, privacy and intellectual property rights. When it comes to on-line speech, the simple reality is that the greater perceived ability for individuals and groups to communicate with each other and with the world at large using the Internet, the greater appears to be present day efforts to control such communications where governments perceive them to be politically undesirable. While there is no question that there are indeed certain types of speech or content which both governments and internet users would find harmful or undesirable and subject to control or even censorship, finding a commonly accepted definition and determination of what exactly that content is, constitutes an impossible feat.

Historically, legal efforts to censor or otherwise control internet "speech" have focused on the key players generally. Each of these has been the focus of varying attempts to censor speech, with varying degrees of success. This paper will examine the evolution of the attempts to regulate speech on the Internet, investigating the role of the key players, focusing on the regulatory solutions implemented by the US and the European Union and evaluating their efficacy. We will also examine the current status of Internet censorship globally as well as the trends for the future especially in view of the increasing concerns over national security, and the loss of economic value to content industries, pushing more countries for legislation to not only control content on the internet, but to enhance the technological ability to actualize such control.

## Freedom of speech: old values in the new (digital) world

### *What does freedom of speech encompass?*

Before determining its scope on the Internet, we must define what is meant exactly by "freedom of speech."[8] Generally, the principle is understood as the freedom of every human expression intended for public communication. This signifies that speech, even speech that causes some measure of harm to the public, is entitled to a special degree of immunity from government restraint. Freedom of speech is a media-independent principle. It originated in a printing press environment[9] and was elaborated on later for the purposes of radio and television.[10]

Free speech clauses developed more or less simultaneously in the United States and Europe. The First Amendment to the American Constitution was adopted in 1791. The Free Speech Clause of the First Amendment to the U. S. Constitution provides that "Congress shall make no law "abridging the freedom of speech."[11] Although directed by its terms to Congress, the clause applies equally to all levels of government.[12]

The European model for the protection of fundamental human rights is based on the existence of two distinct legal orders, namely: the legal order of the European Union ("EU")[13] and the legal order established by the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") within the Council of Europe.[14] The most important provision for European free speech protection is Article 10, ECHR. Its aim is to protect the right of everyone, regardless of frontiers, to express himself, to seek and receive information and ideas, whatever their source, as well as to impart them under the conditions set out in the text of the article 10[15].

"Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without

interference by public authority and regardless of frontiers. This article shall not prevent states from requiring the licensing of broadcasting, television or cinema enterprises."

Similar provisions are found in the constitutions of most democratic states.

### *Restrictions on freedom of speech*

Freedom of speech or freedom of expression is a fundamental right of citizens of the democratic societies. On the other hand, it also generally recognized that this right is not absolute. Free speech has never been completely unrestricted. In the course of time speech has been subjected to various restraints.[16]

In the United States exceptions to free speech rights are not encoded in the First Amendment. Instead, they are to be found in the doctrine of the Supreme Court defining the extent of free speech protection. Some forms of speech are thoroughly outlawed in the US such as fraudulent advertising, child pornography, obscenity, [17] fighting words, [18] libel, [19] speech that infringes a copyright.[20] Naturally, most of these forms of speech have a compelling government interest. Government may regulate, or censor speech if it has a compelling interest, is a public concern, or threatens national safety.[21]

The European framework for government restrictions to free speech is enacted in Article 10, para. 2 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. [22]

"2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

Article 10 of the ECHR, which contains the general conditions for all free speech restrictions, irrespective of the medium they are applied to. According to the text, governmental restrictions to free speech are legitimate only if three cumulative conditions are fulfilled: state interferences restricting free speech must be prescribed by law, they must serve a legitimate purpose and they must be necessary in a democratic society. Every restriction to free speech should be proportionate to its legitimate aim.[23]

### *How the digital environment has affected how we view and exercise our freedom of speech*

The key values that underlie the First Amendment remain the same both in the real and the digital world. As Professor Jack M. Balkin has noted 'the protection of individual freedom to express ideas, form opinions, create art, and engage in research, the ability of individuals and groups to share their views with others, and build on the ideas of others, and the promotion and dissemination of knowledge and opinion remain as important in a world of blogs, search engines, and social software as they did in an Enlightenment era. What has changed, however, is the technological context in which we try to realize these values."[24]

The technological revolution has drastically lowers the costs of copying and distributing information.[25] Large numbers of people can broadcast and publish their views cheaply and widely. Websites, for example, are easy to construct and easy to access. Both receiving and sending information has become easier and less costly.[26] The variety of uses and the potency of the Internet as a form of mass communication are almost unlimited.[27] E-mail's overall volume has already far surpassed that of traditional "snail" mail[28] and constitutes a prime example of the Internet's capacity for fast cheap and efficient means for the expression and exchange of ideas. Other recent developments, such as Web 2.0[29] sites range from social networking sites to virtual worlds, user-generated content platforms, peer produced-public domain encyclopedias, next-generation peer-to-peer file-sharing technologies, enhanced weblogs, and audio and video blogs (also known as podcasts and vlogs, respectively).[30] Features including blogging and YouTube, make it even easier for individuals to express themselves, either in written or video format and reach a larger audience while multimedia friendly interfaces such as MySpace allow users to be heard on a level that never would have been imaginable previously.[31] Social networking sites such as Facebook likewise provide a quick and easy way to stay in touch with friends across the globe. Internet search engines are widely used as the fastest and most effective means of obtaining a wealth of information.[32]

Ultimately, the digital revolution lowered the costs of innovating with existing information, commenting on it, and building upon it by developing common standards for storing and encoding information digitally.[33] Common standards are absolutely crucial to lowering the costs of transmission and distribution because not only do they make it easy to copy and distribute content, they also make it easier to appropriate, manipulate, and edit content[34] promoting thus innovation and creativity.

For the first time in human history content can cross cultural and geographical borders with such ease. Internet speakers can reach more people in more countries; they can interact with and form new communities of interest with people around the globe. The Internet offered people around the world access to an infrastructure for sending information worldwide, a privilege previously enjoyed only by large commercial enterprises.[35]

It has thus been argued that by lowering the costs of transmission, distribution, appropriation, and alteration of information speech has been put in the hand of an large and always increasing number of people from different countries, cultures, diverse backgrounds and strata of society.[36] This participatory nature of the new technologies has contributed to the pluralism of speech thus democraticizing speech worldwide:[37] technologies of distribution and transmission are put in the hands of an increasing number of people and increasingly diverse segments of society throughout the planet;[38] more and more people can publish content using digital technologies and send it worldwide; conversely, more and more people can receive digital content, and receive it from more and more people; equally important, technologies of innovation are available to a wider range of people. In the digital age, distribution and innovation go hand in hand.

Ironically the same aspects of technology that promote speech and innovation also promote and facilitate illegal and harmful acts.[39] The ability to copy and modify information has also led to digital piracy of protected works.[40] The conflict between between intellectual property and freedom of speech always existed, but new digital technologies have made it more salient and important. The web 2.0 raises intellectual property (IP) issues that are similar in kind to, but somewhat more complex than, those raised by more traditional Web and file-sharing technologies. Like the Web 1.0 sites of MP3.com, or Napster that preceded them, sites like MySpace and YouTube stand accused of facilitating the infringement of copyrights in thousands or even millions of songs, television shows, and motion pictures.[41] Copyright holders seek increasingly aggressive ways to protect their existing rights by promulgatin legal and technological strategies seriously affecting freedom of expression.[42]

Internet may facilitate the global communication between peoples of different cultures but it also accentuates the differences in how different peoples value speech. As professor Lessig noted in 1999 every jurisdiction controls speech it deems undesirable but what that speech is, differs from jurisdiction to jurisdiction.[43] This proves problematic in cyberspace[44] as the *La Ligue Contre le Racisme et l'Antisemitisme (LICRA) v. Yahoo! Inc.* [45] case demonstrated in 2000. In this case LICRA and other French organizations against anti-Semitism brought suit in French court against Yahoo!.[46] Plaintiffs alleged that Yahoo!'s auction site was

hosting auctions of Nazi- related materials and memorabilia, the display of which within France violated French law. The French lawsuit, which involved issues of international jurisdiction and choice of law, resulted in a French court order compelling Yahoo! to cease making available the specified anti-Semitic content to French citizens (which at that time essentially required Yahoo! to cease making this content available on the Internet at all).[47]

Yahoo! fought back in the United States by filing a suit in U.S. district court against the French organizations. The company claimed that enforcement of the French court judgment in the United States would violate the First Amendment.[48] The U.S. district court agreed, holding that principles of international comity that would generally favor enforcing international courts' judgment against United States entities were outweighed by the First Amendment values at play in this case.[49] Because the First Amendment protected Yahoo!'s dissemination of anti-Semitic speech, the enforcement of the French court order enjoining such dissemination would violate the First Amendment.[50]

## Myths, Trends and Realities

### *Myths:*

In the early days, the Internet's enthusiasts were convinced that Internet would be basically immune from state regulation. The idea was that even if states wanted to regulate the Net, they would be unable to do so, "forestalled by the technology of the medium, the geographical distribution of its users, and the nature of its content."[51] This belief that Internet is a regulation–free medium can be summarized in the three following assertions:

### Internet cannot be regulated

The famous statement "the Internet treats censorship as a malfunction and routes around it"[52] attributed to John Gilmore, [53] one of the founders of the Electronic Frontier Foundation (EFF), [54] manifests the euphoria generated by the possibilities opened by the Internet. This was true in the nineties and it still holds some truth today mainly because of the technological structure of the Internet.[55] The Internet is basically a distributed de-centralized network, extremely hard to shut down. It appears that if a blockage is put in one place, messages will flow like water around it.[56] This idea reflected the faith in the new technology, which was bound to end censorship and move communications systems away from the control of literacy among the elite and towards multiple forms of communications.[57]

## Information wants to be free

Much like Gilmore's assertion above, Stewart Brand's phrase "information wants to be free"[58] further visualizes the idea that he Internet is incapable of being regulated not only because of the technology, but also because of the nature of the messages, the content, communicated through it. Internet was viewed as the ultimate communications medium which would allow ideas to "freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, [...] like fire, expansible over all space, without lessening their density at any point, and like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation."[59] On the one hand Internet is a realm of information, and information is very hard to regulate; on the other hand states are too slow to deal with the technology and thus control information.[60]

## No single state can regulate speech on the internet

The third basic belief is reflected in John Barlow's phrase, "On the Net, the First Amendment is a local ordinance." The idea was that proponents of freedom of speech, should not put their faith in the law to protect free speech; instead they should put their faith in technology.[61] It is the nature of the network technology, the nature of the informational content, and the fact that it stretches across borders beyond the control of any one sovereign all mean that speech cannot be regulated. In sum it is exactly the global nature of the Internet that is global, that is rendering it impossible for individual states to regulate speech.[62]

### *Realties: controlling the who, the what and where?*

### Generally

As we all know by now Internet can and is in fact regulated by individual states.[63] Professor Pamela Samuelson had warned as early as 1996 that the law was already threatening an important regulation of life in cyberspace.[64] Indeed, in the past years there has been a gradual change of the techno-political culture of the Internet from a cheap, effective, and global distribution network to a state driven regulated entity. [65] This is partly due to the shared concerns of many countries to exert control over the information flow for various compelling state reasons;[66] the motivations for censorship range from well-intentioned desires to protect children from unsuitable content[67] to authoritarian attempts to control a nation's access to information.[68]

## Methods of content regulation

Professor Lessig has described the Internet in terms of the end-to-end (e2e) principle.[69] The e2e principle views the Internet much like a common carrier, simply serving as a neutral conduit for information flowing from the content provider, or "speaker," on one end to the end user receiving the information, or "listener," on the other end, [70] while it also requires that all data packets, or bundles of information, should be treated equally as they pass through the middle of the network, regardless of their content.[71] This principle, albeit consistent with the notion of the Internet as a forum promoting First Amendment freedoms[72] is not applicable in practice. The various methods of Internet content regulation developed are not always consistent with the e2e principle.[73] There are two major of the methods of content control on the Internet content, distinguishable based upon the location on the Internet where the regulation occurs.

### *End users*

This method consists of regulating who are sending data packets and who are receiving them. This approach involves state-mandated controls at the end-points of the network. On the one hand, states have sought to block illegal or harmful content at its source[74] by making it illegal to send such harmful information.[75] In this sense this approach acts proactively by prohibiting Internet users from disseminating certain information or message over the Internet. In the US such examples include the Communications Decency Act of 1996, [76] which sought to stop the transmission of pornography to minors, and the CAN-SPAM Act of 2003, [77] which disallows the sending of unsolicited commercial e-mails if certain rules are not followed.

On the other hand there is state regulation which attempts to control the receiving end of the communication by prohibiting the receipt or possession of specific content such as child pornography or copyrighted works.[78] The on going battle of the music and movie industry against internet users and P2P file sharing constitutes the prime example of attempts to control file sharing on the end user level. The industry's legal battle against individual file sharers spanned roughly five years, targeting more than 35, 000 alleged file sharers in the U.S.[79] As of this writing, only two cases against individual file sharers have actually gone to trial. In *Capitol Records v. Thomas*, [80] resulted in an arguably Pyrrhic victory for the music industry plaintiffs. The Recording Industry Association of America ("RIAA") won the case on the merits in two separate trials.[81] In the retrial, the jury found against Thomas again, this time awarding $ 1.92 million, or $ 80, 000 per song, in damages. Although the district court "remitted the damages award to $2, 250 per song" in January of 2010, Thomas-Rassett nonetheless still faced a "reduced

award" in the amount of $54, 000, that is, in the court's own words, "significant and harsh."[82] In *Sony Corp. v. Tenenbaum*[83] the jury awarded the RIAA $ 675, 000, or $ 22, 500 per song.[84] On December 7, 2009, Judge Gertner finalized the verdict against the defendant and issued an injunction preventing him from file-sharing, but still permitted him to speak publicly about his trial.[85] The Rasset-Thomas case was the first major victory against individual file-sharers for the RIAA, which has been trying to stop file-sharing for the past ten years.[86] However, this campaign has undoubtedly proved costly and critics largely viewed the litigation as ineffective[87] damaging the reputation of the industry, widely seen as one that sues its own customers and out of step with current technology.[88] As a result in December 2008, the RIAA announced that it would no longer pursue litigation as a means of combating illegal file-sharing, although it would continue to litigate any outstanding cases.[89]

A middle of the road approach includes regulations mandating that certain content be accompanied by specific information in order to be legally sent or received. Examples of this type of regulation include again the CAN-SPAM Act which requires that certain header information is included in some messages.[90] Also, the Children's Online Privacy Protection Act of 1998 (COPPA)[91] requires that web sites implement age verification methods which prohibit Internet users from accessing certain information online unless they provide verify that users are over thirteen years of age before providing most online services. None of these first three approaches necessarily represent a substantial departure from the end-to-end principle, so long as no intermediaries, such as Internet service providers (ISPs), are required to take any action on behalf of the state to enforce the rules.

*Internet Service Providers*

Following the admittedly unsuccessful attempt to control the end users, there has been a shift in the targets that are subject to regulation.[92] Rather than holding the actual speakers or writers to be legally liable for uttering or expressing undesirable speech, [93] the intermediary carriers in the Internet age who have no actual knowledge of the content may also be liable.[94] Their crucial role in content regulation is inevitably associated with the architectural design of the Internet. Indeed there is only a limited number of Internet companies which possess the power to offer online services. In contrast, all users must go through an ISP before going online. Due to the setup of the Internet, the Internet Service Providers ("ISPs") are situated in this powerful and influential position making them the perfect target for state-mandated regulation and/or self-imposed content censorship.[95] Because of pivotal role ISPs play in content regulation we shall examine their role in more detail.

## Safe harbors

It has to be noted that because of the Internet's unprecedented speech-facilitating characteristics and the pivotal role that Internet Service Providers play in channeling such speech the issue of shielding ISPs from liability based on the third-party generated content-especially in the area of copyright law- arose early. Although internationally, a multinational treaty directly addressing the issue of ISP safe harbors does not exist, numerous domestic regimes which reject strict liability for safe harbors so long as ISP's are not directly involved in the creation of the illegal or censored content are implemented. For instance Section 230(c)(1) of the Telecommunications Act of 1996 provides that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[96] Accordingly, Internet intermediaries like network providers and online service providers but also websites or online services on which other people provide content (chat rooms, blogging services, website hosting services, search engines, bulletin boards, or social networking sites like Facebook and Myspace, cannot be held liable for what other people say when others use these networks, services, or sites.[97] This privilege applies to a wide range of different communications torts and crimes but not to alleged infringements of intellectual property rights. In these cases, the safe harbor provisions of the Digital Millennium Copyright Act apply.[98] Under the DMCA, no copyright action may lie for damages against companies providing Internet connectivity or transmitting or routing material over the Internet provided the ISP is not involved in the creation of the content in question.[99]

Similarily, in the European Union the Electronic Commerce Directive (ECD) erects safe harbors for online intermediaries.[100] Under the ECD providing access to a computer network or transmitting information over it, including engaging in the transient storage or reproduction of the information for transmission, shall not give rise to monetary liability irrespective of notice of illegal activity[101] as long as "[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 ... upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."[102]

## Government mandated regulation

One of the most effective methodologies to control internet content to date appears to be placing pressure on the internet service provider. Unlike the attempts to regulate thousand or even millions of end users, ISPs are likely to provide effective, efficient, and economic means of control. As a result, ISPs are enlisted to

block or to inspect packets of information.[103] On the other hand, the corporations find themselves required to comply with rules in jurisdictions in which they are doing business and whose views on freedom of expression may be entirely different from their home countries.[104]

## ISPs as state-mandated censors

The most common method to regulate undesirable content on the Internet is through Internt filtering.[105] This is the original and best understood form of Internet censorship. Internet users on a particular network are blocked from accessing specific websites.[106] Internet filtering generally describes technical approaches to control access to information on the Internet. There are three commonly used techniques to block access to Internet sites: IP blocking, DNS tampering, and URL blocking using a proxy.[107] These techniques are used to block access to specific WebPages, domains, or IP addresses.[108]

However, there are two inherent flaws associated with all internet filtering technologies: underblocking, in which case the filter is simply ineffective, and overblocking, when the technology implemented blocks content it did not intend to block.[109] The problem lies within the limitations of the current technology[110] since current technology is not able to accurately identify and target specific categories of content found on the billions of web pages and other Internet media[111] often resulting in blocking unrelated websites. In reality, when ISPs are required by state regulations to filter objectionable materials, they have to respond quickly and tend to adopt the cheapest means to do so, resorting to filtering by IP address.[112] However the unintended consequence is that if the target Web site is hosted in a shared hosting server, all websites on the same server will be blocked[113] resulting in filtering out numerous unrelated web sites.[114] For instance, South Korean ISPs were required to block thirty-one web sites by the authorities, but in choosing to block by IP address, 3, 167 unrelated domain names hosted on the same servers were blocked as well.[115] This problem of over-blocking by ISPs' has been described by Zittrain as a crude form of Internet discipline, amounting to a form of "Internet death penalty."[116]

China is notorious for having implemented the most sophisticated system of Internet censorship and surveillance in the world.[117] The 'great firewall of China' uses a variety of overlapping techniques for blocking content containing a wide range of material considered politically sensitive by the Chinese government. While China employs filtering techniques used by many other countries, including DNS (domain name system) tampering and IP (internet protocol) blocking, it is unique in the world for its system of Internet connections when triggered by a list of banned keywords. Known as a TCP reset, this content filtering by keyword targets content regardless of where it is hosted.[118] Any foreign internet company wishing to penetrate the immense Chinese market have to adhere to the strict

content regulation requirements mandated by the Chinese government[119] and internet giants such as Google, Microsoft and Yahoo! are no exception.

As a result, Internet users in China have access to a "sanitized" version of search results.[120] The type of content that is targeted for blocking is wide-ranging and covers social, cultural, security and political topics considered a threat to Communist Party control, and social and political stability.[121] Websites that are almost always filtered include the ones containing content related to Taiwanese and Tibetan independence, Falun Gong, the Dalai Lama, the Tiananmen Square incident, opposition political parties or a variety of anti-Communist movements[122] but also the web sites of major news organizations, such as the BBC, as well as international advocacy organizations, such as Human Rights Watch.[123] Up until recently a search request for the Tiananmen Student Movement at Google.com would yield pictures of rolling tanks, whereas only smiling faces of passers-by would appear at Google.com.cn.[124] As a Citizen Lab[125] study of four popular search engines in China found, the total number of censored sites may not be that high, especially when compared to the amount of indexed sites, however the impact of their exclusion cannot be underestimated since the censored sites are often the only sources of alternative information available for politically sensitive topics.[126] Without knowing what has been filtered and the alternatives available, users are forced into a "digital deceit,"[127] without even realizing that they are living in different Internet universe.

Until recently Google defended its practices in China arguing it would do more harm than good to not participate in countries notorious for their hostility to free speech.[128] However, this changed in early 2010 when Google announced its decision to stop operating in China.[129] Specifically, in January 2010 Google decided to stop censoring search results in China, after discovering that someone based in that country had attempted to hack into the e-mail accounts of human rights activists.[130] Although no direct accusation against the Chinese government was ever made, Google stated that the attacks, combined with attempts by China over the last year to "further limit free speech on the web," led it to conclude that it needed to "review the feasibility of [its] business operations in China."[131] In March 2010 Google shut down its Google.cn site and has been redirecting users to Google.com.hk, where it offers uncensored Chinese-language search services.[132] While Google ended its own self-censorship in China, searches within the .hk Google, albeit not censored by Google, will still be affected by China's keyword filtering, i.e. searches for certain terms will not get through to google.com.hk search engine and the end user in China will not get any results.[133] The difference is that the user now experiences the censorship first hand.[134] Despite Google's rhetoric about protection of freedom of expression in China it is ques-

tionable whether the company would have decided to stop its operation in China had it not been the victim of the December 2009 cyber-attacks.

Apart from filtering there are several instances where governments get involved directly requesting removal of specific content. Indeed since the infant stages of the internet government have called upon ISPs to removing undesirable content. For instance, in 1995, the German Government requested CompuServe to remove porn sites from its servers a request to which Compuserve ultimately complied by implementing a content filtering scheme on a country-by-country basis.[135] Similarly in 2001, Google removed pro-Nazi and racist sites from search results in its localized search engine, following requests of the French and German governments.[136]

In 2008, following a civil court judgment in Civril, Turkey access to a photo and media-sharing service, Slide, closed to all Turkish citizens because some material deemed insulting to the country's founder, Ataturk, was posted.[137] The same year, the Indonesian government ordered the country's internet service providers to bock YouTube for publishing the 15-minute anti-Muslim film "Fitna", made by Dutch MP Geert Wilders, leader of the anti-immigration Freedom Party (PVV). Some of the country's ISPs followed the block order, but "Fitna" could still be viewed through other providers.[138] That same year following riots in Tibet, China shut down access to YouTube inside the country in an effort to contain the news.[139] In late February 2008, Pakistan's telecoms regulator ordered a ban of You Tube after a "blasphemous" speech critical of Islam was posted. Pakistan's blocking of YouTube was so effective that disabled access to the popular site everywhere in the world for a few hours.[140] More recently, in May 2010 Pakistan imposed a ban on the social networking site Facebook amid anger over a page that encouraged users to post images of Islam's Prophet Muhammad.[141] This ban was lifted only after officials from the social networking site apologized for the offensive to Muslims page and removed its contents.[142]

## ISPs as State-Informers

A more troubling trend is that increasingly state governments rely on ISPs to retrieve information about internet users, thus employing ISPS as informers or the "secret police" of the Internet.[143] A few of the most notorious cases of corporate involvement in assisting the a government arresting and condemning four dissidents — Shi Tao, Li Zhi, Jiang Lijun and Wang Xiaoning — to prison for terms of up to 10 years involves Internet giant Yahoo!

In 2004 Yahoo, turned over information about the Chinese journalist, Shi Tao, to the Chinese authorities.[144] In April 2004 Shi Tao used an anonymous identity to send by his Yahoo! email account[145] the content of "A Notice Regarding Current Stabilizing Work" to the "Asia Democracy Foundation" in New York.[146] The con-

tent of the document essentially warned journalists that overseas pro-democracy Chinese dissidents may come back to mainland China during the 15th anniversary of the Tiananmen Square Protests of 1989 on June 4, which would affect the politico-social order's stability and asked all news media to not report anything regarding the so-called "June 4th event", Falun Gong or people calling for politico-social change. The Chinese government obtained the account holder's information, which described the IP address, the corresponding user information, Shi Tao's telephone number, and the location of his terminal, by Yahoo! (Holdings) Hong Kong Ltd. ("Yahoo! (HK)")[147]. In April 2004, charged with the offence of illegally providing state secrets outside the country in violation of Article 110 of the Criminal Code of the People's Republic of China ("PRC").[148] On April 30, 2005, Shi was sentenced to ten years imprisonment.[149]

Yahoo! defended itself, stating that it had not betrayed its users, but that it had to operate within the law, regulations, and customs of the country in which it is based or else it would have no alternative but to leave the country.[150] Some months later, it was discovered that the document provided to Yahoo! China on April 22, 2004 by the Beijing State Security Bureau actually stated, "Your office is in possession of the following items relating to a case of suspected illegal provision of state secrets to foreign entities..."[151] directly contradicting the sworn Congressional testimony by Yahoo! Senior Counsel Michael Callahan in February 2006.[152]

After Shi Tao's story attracted publicity world-wide three other cases in which Yahoo! provided information to Chinese authorities about people who used Yahoo! China e-mail accounts to transmit political information were revealed: Wang Xiaoning, a Chinese engineer by profession, who posted electronic journals in a Yahoo! Group calling for democratic reform and an end to single-party rule;[153] Li Zhi, a former government worker who criticized the Communist Party in online discussion groups and encouraged others to join the China Democracy Party;[154] and Jiang Lijun, a Chinese freelance writer who posted articles on the Internet advocating a multiparty system of government . All were tried and sentenced in 2003 – one year before Shi's arrest. In all three cases, Chinese court documents cite Yahoo! Holdings (Hong Kong) as the source of information about the defendants' Chinese Yahoo accounts.[155]

On August 28, 2007, the World Organization for Human Rights USA sued Yahoo! under the Alien Tort Statute for Xiaoning' alleging that Yahoo! "knowingly and willfully aid[ing] and abett[ing] in the commission of [plaintiffs'] torture" by providing the Chinese authorities with information, including plaintiffs'e-mail records IP addresses and user identification numbers, that caused the arrests of writers and dissidents.[156] On November 13, 2007, Yahoo!, Xiaoning, along with

Shi Tao, who was later named as an additional plaintiff, settled the lawsuit for an undisclosed amount[157] leaving questions raised about corporate liability unanswered.

Similarily, in 2007, Google was alleged to have handed information of its user, who had posted insulting images of god Shiva on its social networking site, to the Indian government. Ironically, Google passed the wrong information to the authority, leading to the arrest of an innocent person.[158] Again in 2008, a 22-year-old tech worker in a suburb of Delhi, posted on a comment titled "I hate Sonia Gandhi" in an Orkut community through an Orkut account associated with his Gmail account. Law enforcement immediately took action and Google not only did it take down the material but also gave the user's IP address to police, allowing them to track down his physical location leading to the user's arrest.[159] Google wouldn't disclose what precisely was posted about Ms. Gandhi, but said it determined the material violated India's obscenity laws.[160] The company said it supported the free expression of its users and is committed to protecting user privacy, but the company complies with local laws and valid legal process, such as court orders and subpoenas.[161]

In 2006, in United States, a country famous for its liberal views on freedom of speech, it was revealed that AT&T was cooperating with the National Security Agency surveillance program of the U.S. Government to monitor communications of its citizens with suspected terrorist ties outside of the United States.[162] The Electronic Frontier Foundation ("EFF") sued the telecommunications company on behalf of its customers for violating privacy law by collaborating with the NSA in the massive program to wiretap and data-mine AT&T's users' communications. In June 2009, a federal court dismissed this and dozens of other lawsuits against telecoms, ruling that the companies had immunity from liability under the controversial FISA Amendments Act (FISAAA), which was enacted after the filing of the case.[163]

Google has had its own battles with the government. In August 2005, the U.S. government ordered the company to comply with a subpoena that would provide "a multi-stage random sample of one million URL's" from Google's database, and a computer file with "the text of each search string entered onto Google's search engine over a one-week period (absent any information identifying the person who entered such query" to implement the Child Online Protection Act.[164] In the end, the Justice Department came to a compromise by requesting merely fifty thousand URLs and five thousand search queries, and finally only looking at ten thousand and one thousand, respectively[165] which also raises a question about the arbitrariness of the initial request.

Although it is well known that communications or customer records that are in storage by third parties, such as email messages, photos or other files maintained in the cloud by services like Google, Microsoft, Yahoo Facebook and MySpace are routinely disclosed to law enforcement, and there is no legal requirement that statistics on these kinds of requests be compiled or published.[166] As a result, there is currently no way for academic researchers, those in Congress, or the general public to determine how often most email, online photo sharing or social network services deliver their customers' data to law enforcement agents.[167] Security and privacy analyst Christopher Soghoian filed Freedom of Information Act requests with several parts of the Department of Justice in the summer of 2009, in an attempt to follow the "money trail" in order to determine how often Internet firms were disclosing their customers' private information to the government.[168] Comcast and Cox did not object but both Verizon and Yahoo! resisted disclosure of such information. Verizon first revealed in its objection letter that it "receives tens of thousands of requests for customer records, or other customer information from law enforcement" and claimed among others that its customers might "become unnecessarily afraid that their lines have been tapped, or call Verizon to ask if their lines are tapped."[169] Yahoo! claimed that if such information is disclosed "would be used to "shame" Yahoo! and other companies -- and to "shock" their customers" and impair the company's reputation.[170]

Finally in April 2010 Google announced the launch of the new Government Requests tool[171]"to give people information about the requests for user data or content removal received from government agencies around the world" stating the belief that this tool will promote "greater transparency", will enable discussions about the appropriate scope and authority of government requests and that other companies will make similar disclosures.[172] Although there are limits to what this data actually discloses to the public[173] it is an imperfect yet significant step toward transparency.

## Private censorship or self-regulation

Besides government mandated regulation Internet providers customarily proceed to content restrictions amounting to self-regulation, in other words a form of private censorship. The vast majority of Internet access and service providers, which are privately owned, assert and exercise substantial control over the expression that flows through their conduits.

First there is a matter of transparency with regards to the specific criteria used in the different filtering regimes.[174] Since one of the flaws of filtering regimes is overblocking, collateral filtering albeit unintended, necessarily means that both the ruling authorities and the public may not even know what has actually been filtered, rendering commercial companies who have the technical know-how to

the ultimate decision makers.[175] Moreover, since most companies consider and treat commercial filtering technology and block lists as the intellectual property of the manufacturers and ISPs, to which the public cannot have access[176], the chance of challenge is minimal. As a result there is practically no accountability for the ISPs filtering practices which maybe vague and arbitrary.[177] In essence ISPs are in a position which allows them to broadly restrict access to the Internet which in turn means that the ISPs are in fact determining who can be online, what can be viewed, and who can say what is on a what was originally considered a free-for-all medium.[178] Taking this into account it arguable that ISPs are no longer mere conduits or neutral intermediary carriers.[179]

Transparency is equally absent in the way search engines work. Search engines occupy a position of central importance on the Internet.[180] The percentage of internet users who use search engines on a typical day has been on rise since 2002 estimating that the number of those using a search engine on a typical day is closer to the 60%[181] and the major search engines, Google and Yahoo!, and Bing ranked as the three most used websites in the United States.[182] The rise in the importance of search engines in online communications is reflected in the increased litigation involving demotions in the website ranking or search engine's refusals to include advertisements.[183] The importance of search engines is also reflected in the energy that webmasters put into ensuring that they are included in search engine indices and in attempting to improve their ranking within search results.[184] Certain forms of bias seem inherent in the structure of the search engines. For instance when search engines build their indices using automated software agents ("bots") which follow hyperlinks between websites, [185] and search engines use the number of links to a site as a proxy for its quality, [186] the link structure of the Web may favor popular and highly-linked sites.[187] However, most of the debate focuses different forms of bias introduced by search engines, including the removal of websites from the search engine index, the reduction of website ranking, the refusal to accept keyword-triggered advertisements from certain websites, and the practice of providing preferences in indexing or ranking for paying websites.[188] Several authors have noted the problem of bias in search engines, although they differ widely in their recommended solutions.[189] Several have called for a transparency requirement to be imposed on search engines. This transparency requirement should include (a) disclosure of the way in which the search engines work and how they rank search results, [190] (b) clear identification of paid links, [191] and (c) notification when information is blocked or removed pursuant to law.[192]

Secondly, each of the major ISPs establishes and enforces Terms of Service by which it sometimes prohibits the expression of certain types of speech that are considered protected speech. AOL, for example, specifies in its terms of Service

that AOL and its agents "have the right at their sole discretion to remove any content that, in America Online's judgment ... [is] harmful, objectionable, or inaccurate."[193] AOL enjoys the discretion to censor constitutionally-protected speech in its discussion forums and other online spaces, including "vulgar language or sexually explicit conduct" that it describes as being as appropriate as they "would be at Thanksgiving dinner" and warns that AOL makes the final determination about whether content is objectionable or not.[194]

Similar restrictions on speech are imposed by most if not all major ISPs making practically impossible for Internet users seeking stronger protection for their expression to "shop around" and chose a different ISP. For Instance Yahoo!'s Terms of Service,[195] prohibit users from making available content that is "objectionable," and warns that Yahoo! may pre-screen and remove any such "objectionable" content.[196] Comcast prohibits users from disseminating material that "a reasonable person could deem to be objectionable, embarrassing, ... or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful."[197] also stating in its Terms of Service, that it "reserves the right ... to refuse to transmit or post and to remove or block any information or materials ... that it, in its sole discretion, deems to be ... inappropriate, regardless of whether this material or its dissemination is unlawful."[198]

Internet Providers policies may also further restrict free speech. In 2008 Google was accused that its "excessively restrictive policies" have resulted in the censorship of lawful advertisements that educated and informed the public.[199] An activist who wished to place an advertisement stating "AT&T has given $7, 500 since 2004. Who else has donated to the senator?" to be displayed when Internet users searched for the name of a particular politician was censored by Google. Google informed the user that the ad campaign run for the previous months was being terminated due to a trademark complaint by AT&T.[200]

In the United Kingdom, Google was reported to have 'delisted' Inquisition 21st Century, a website campaigning against many of the Operation Ore child pornography convictions in the UK suggesting Inquisition 21 had attempted to manipulate search results.[201] In 2008, Google refused to run ads for a UK Christian group opposed to abortion, explaining that "At this time, Google policy does not permit the advertisement of websites that contain 'abortion and religion-related content."[202]

Profesor Dawn Nunziato cites several more examples, including Google's suspension of ads for W. Frederick Zimmerman, once it became aware of the content of the author's book - Basic Documents About the Detainees at Guantanamo and Abu Ghraib - advertised via his sponsored link.[203] Google cited its policy not permiting "the advertisement of websites that contain "sensitive issues"; Google's

suspension of ads for a website that contained an article criticizing President Bush on the ground that ads advocating against an individual violate its polic; Google's refusal to run the ad of Unknown News for anti-Iraq-war bumper stickers on Google's Sponsored Links with an ad headlined "Who Would Jesus Bomb?". Google finally agreed to reinstate it if the website was edited ""to show both sides of the argument' over attacking Iraq."[204]

Third, network providers might discriminate the content and applications of favoring some speakers and businesses over others by blocking access to certain[205] sites and services or permit access to end-users only if these sites or services pay a special fee.[206] Major Internet companies including Google, AOL, and EarthLink exercise great editorial control and impose what in essence is speech regulations especially with regards to sponsored links.[207] Google is known for having refused to host a range of politically-charged, religious, and critical social commentary in the form of advertisements themselves, as well as the websites to which these advertisements link. Google has also required prospective advertisers to alter the content within their sponsored links - as well as within their websites - as a condition for Google's hosting such content. One of the most notorious cases involve Google when in 2002 it removed websites critical of the Church of Scientology. This incident sparked numerous complaints from Internet users and groups to Google, and the links to the banned site were restored.[208] Google subsequently began to contribute its notices to chillingeffects.org, archiving the Scientology complaints and linking to the archive. However more cases soon followed. For instance in 2003, Google stopped showing the advertisements of Oceana, a nonprofit organization protesting a major cruise ship operation's environmental policies under the headline "Help us protect the world's oceans," citing its editorial policy at the time, stating "Google does not accept advertising if the ad or site advocates against other individuals, groups, or organizations."[209]

Additionally, Internet providers might seek to control certain heavily trafficked sites - like eBay, Google, or sites that use considerable bandwidth[210] to ensure that their traffic flows smoothly to end-users.[211] In 2007, after independent testing by the Associated Press, later confirmed by EFF, it was discovered that Comcast began engaging in protocol-specific interference with the activities of its subscribers, specifically with BitTorrent, Gnutella, and potentially other common file sharing protocols employed by millions of Internet users.[212] Comcast claimed that it performed "network management" that might interfere with particular subscribers in rare circumstances, but it did not block or target any application or protocol.[213] The Federal Communications Commission (FCC), intervened and asserted jurisdiction over Comcast's network management policies and ordered Comcast to cease discriminating against peer-to-peer network traffic. On April 6, 2010, the DC Court of appeals in a unanimous three panel decision vacated the Federal Communica-

tion Commissions's 2008 order against Comcast.[214] The Court did not reach the question of whether Comcast had wrongfully interfered with its subscribers' use of internet services like file sharing and Skype; instead, it held that the F.C.C. lacks statutory authority to regulate broadband services. According to news reports, the court's decision will make it more difficult to enact legislation safeguarding net neutrality.[215] Following this decision, the FCC announced that it was "seriously considering" placing the internet industry in the same category as the telecommunications industry, a highly regulated industry that will further limit ISP neutrality.[216] Many are concerned with the potential ramifications of such a reclassification. On May 2010 a group of 171 House Republicans May 28 sent a letter to Federal Communications Commission Chairman Julius Genachowski protesting a plan to reclassify broadband internet access as a "telecommunications" service.[217]

This decision sparked once more the debate about net neutrality. The principle of network neutrality holds that, in general, network providers may not discriminate against content, sites, or applications.[218] The goal of network neutrality is to keep digital networks open for many different kinds of content and for many different types of applications and services that people may devise in the future.[219] But when talking about the role of Internet or network providers in the debate over network neutrality, we have to realize that discrimination against certain types of content or services is not so much based on their politics or their moral tone (although there have been exceptions).[220] Most ISP-imposed discrimination will be for economic reasons - to favor business partners and protect their business models.[221] Internet providers might want to give a traffic advantage to their content partners or to their own content, [222] reserving a fast track for favored content partners; conversely, network providers would not protect the flow of content (or even slow down content) from non-partners, competitors, amateurs, and end-users.[223]

Probably the most ironic instance of self-censorship, arguably based on business considerations, is Yahoo!'s case against La Ligue Contre le Racisme et l'Antisemitisme. After Yahoo! won a highly publicized international battle on behalf of free speech values in *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, [224] Yahoo! chose, apparently based on commercial considerations, to prohibit the dissemination of the Nazi-related content at issue in the case.[225] Other U.S based Internet search engines and service providers also refuse to host Nazi-related and other controversial content, even though such speech is protected by the First Amendment against government censorship.[226]

## Current Trends: putting the pressure on ISPs

The analysis above demonstrates the ways in which private entities, including Internet providers like Google, AOL, and Yahoo!, have broadly exercised the power

to regulate and censor speech on the Internet.[227] These companies serve as conduits for the speech of others since internet users depend on them for access to other speakers[228] making them the ideal point of control for restricting online speech.

Probably the most prominent attempt at censoring content on the internet stemmed from the battle of the music industry against peer to peer file trading. That conflict has always existed, but new digital technologies have made it more salient and important.[229] This battle continues to this day and the music and movie industry has been the driving force in introducing and implementing speech regulations throughout the world. Like most of the developments involving the protection and censorship of speech on the internet there is both positive and negative results. On the one hand most jurisdictions have implemented safe harbors for internet service providers[230] shielding them from liability for the actions of their end users, so long as they were not actively involved in the posting or dissemination of the allegedly illegal content beyond the mere provision of services. On the other hand the same developments have also affected adversely speech.

### *Copyright v. anonymity*

The first step in restricting infringement of intellectual property rights is to identify the infringer. Thus the Music industry promoted early the adoption of legislative regimes which would facilitate identification of the alleged infringer. In United States, the copyright owners have a critical weapon in their arsenals recent against illegal sharing of copyrighted work, the abbreviated subpoena procedures established in Section 512(h).[231] Under Section 512 (h) copyright owners have the ability to obtain a subpoena on request from a clerk of a United States District Court for disclosure by a service provider of the identity of a subscriber who has allegedly engaged in copyright infringement.[232]

Unlike the notice and take down provisions of Section 512(c), [233] there is no requirement that subscribers whose identity is being sought be notified of the subpoena or given an opportunity to challenge its propriety prior to disclosure of their identity.[234] Moreover, such subpoenas are issued as a ministerial act of the clerk of the court, without the need for, or benefit of, judicial oversight.[235] Following the court decisions in the *Recording Industry Ass'n of America, Inc. v. Verizon Internet Services*,[236] where the court held that §512(h) applied only to ISPs that stored infringing data on their servers, not ISPs that acted solely as intermediaries[237] RIAA's ability to use § 512(h) to obtain contact information about accused infringers was limited forcing RIAA to commence what became known as its "John Doe" lawsuits.[238]

In Europe, the European Court of Justice also struggled with the communication of personal data in the context of civil proceedings.[239] In the famous case

of *Promusicae v. Telefonica de Espana SAU (Telefonica),*[240] Plaintiff, Promusicae, a Spanish consortium of music and video producers, requested that Spanish ISP Telefonica reveal the identity of certain subscribers suspected of illegal file-sharing. After a Spanish court granted the request, Telefonica filed an appeal arguing that European law barred it from sharing personal data with Promusicae.[241] The Spanish Court of Appeal in Madrid referred the matter to the European Court of Justice on the issue of whether Promusicae violated EU law. The court considered whether, under Council Directive 2004/48 on the enforcement of intellectual property rights, and Articles 17(2) and 47 of the Charter of Fundamental Rights of the European Union, member states must require ISPs to disclose personal data to third parties in cases involving copyright violations. The court held that there is no such requirement.[242] The ECJ ruled that Member States have no obligation to require an ISP to disclose information to a rights holder in civil proceedings.[243] The ECJ left the decision to be balanced between the competing rights of intellectual property rights and privacy rights.[244] In the end the ECJ noted that the obligation to protect right holders private information should not be leveraged or expensed against the cost of data protection[245] invoking the principle of proportionality in urging member states to strike a fair balance among the various fundamental rights protected by the Community legal order.[246]

### *Three strikes or graduated response scheme*

### Legislative Provisions

The RIAA's campaing against individual users, also known as the "John Doe' campaign, proved largely unsuccessful and generated a lot of bad publicity for the music and movie industry. As a result, this industry adopted a new response: the graduated response plan, which threatens users with the possibility of losing their access to the Internet, rather than with the threat of lawsuits.[247] This approach, known as the "three strikes"[248] or graduated response plan, [249] involves both the music industry and the ISPs. The music industry monitors and notes IP addresses of alleged infringers and notifies the respective ISPs.[250] In turn, ISPs then contact the users and give them three chances to stop their infringing activities.[251] Failure to comply with the warning to stop, will result in the ISP's suspending the users' Internet access through the ISP's server.[252] In order for the RIAA's new anti-piracy initiative to succeed, the RIAA needs cooperation from regional ISPs.[253]

In the United Sates, if ISPs do not agree to implement a graduated response plan, however, the RIAA could compel them to comply by invoking 17 U.S.C. § 512(j)(1)(A)(ii). This subsection of the DMCA permits the copyright holder, to go to court and get:

"an order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order."[254]

Although the copyright holder must get a court order to terminate Internet access, a preliminary injunction can be issued without a trial.[255] In addition, the injunction is issued against the ISP, rather than the user thus depriving the end –user his or her day in court.[256] ISPs who refuse to cooperate which might also be threatened with liability, under § 512(j).[257] Section 512(j) thus creates a system where copyright holders can get an "extra-judicial temporary restraining order, based solely on the copyright holder's allegation of copyright infringement."[258] The music industry's new initiative has been more successful in Europe where it has resulted in the adoption of legislation incorporating and implementing the graduated response plan. In 2007 the French government requested a commission led by Denis Olivennes to negotiate an agreement between organizations representing the music and film industry and internet service providers on proposals to combat unlawful file-sharing.[259] This process resulted in a controversial legislation known as HADOPI, named after the government agency created by the resulting law (Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet)[260]. The purpose of this bill was to implement a so-called *riposte graduée* or graduated response. Upon request on behalf of the copyright owner, HADOPI would request that the relevant ISP to provide the contact details of the subscriber whose IP address is under investigation and send an email recommendation to the subscriber concerned advising the user of the danger of acts of infringement and of the existence of security devices. If, during the six months following this first recommendation, similar violations are recorded, a second recommendation may be sent by letter with acknowledgement of receipt. Failure to comply would enable HADOPI order suspension of internet access for the user in question. This last provision caused the Constitutional Council's to strike down the original HADOPI law.[261] Council reasoning that only a judge may order the suspension of internet access not an independent administrative authority such as HADOPI.[262] Soon thereafter, the French government proposed HADOPI 2 to Parliament instituting a judicial process[263] prior to ordering internet suspension but essentially keeping the main provisions of the original law intact. HADOPI 2 passed constitutional muster on October 28, 2009.

Similar to HADOPI Law, the United Kingdom, recently enacted the Digital Economy Act.[264] Under this act, passed on April 8, 2010, [265] ISPs will be required to send warning letters to any individual users suspected of illegally downloading copyrighted files after receiving sufficient evidence from a copyright holder that unlawful copyright infringement is taking place.[266] Ofcom, which regulates the

UK's broadcasting, telecommunications and wireless communications sectors, is given the authority to take tough measures combat unlawful P2P file sharing. The Digital Economy Act empowers Ofcom to use tougher measures to combat unlawful P2P file sharing. If a system of warning letters to alleged pirates fails to reduce online infringement substantially within 12 months, [267] Ofcom can then have ISPs hand over the alleged infringers' names and addresses so the copyright holders can serve them with a court injunction. ISPs can also be required under the new law to implement technical penalties, such as reducing Internet download speeds, blocking web sites, and suspending internet access to individual users.[268] However, following strong critism[269] and after public pressure it has been speculated that the coalition government taking over in the UK, some may decide to repeal or modify the Digital Economy Act.[270]

Other countries are also in the process of introducing similar laws. New Zealand after an initial unsuccessful attempt to pass its own version of "three strikes" law in 2008[271] returned with an updated version of the law in 2010.[272] On March 2010, Belgian senator Philippe Monfils presented a new version of his proposition for a law that would implement in Belgium the graduated response system in illegal downloading cases, as the one introduced by the Hadopi law in France. The Belgium draft law includes blocking of websites via ISP, similar to the French system introduced by Hadopi law.[273] Similar laws and policies have been considered even if ultimately rejected by by Australia, Hong Kong, Germany, the Netherlands, South Korea, Sweden and Taiwan.[274]

## Voluntary Collaboration

To achieve efficiently function of the graduated response plan the copyright holders must have the full cooperation of ISPs in withholding services from repeat infringers. The reaction of ISPs seem to vary between acceding to the RIAA's demands for fear of being found contributory liable, and protecting users' rights and their own business interests.[275] AT&T, a large ISP, agreed to work with the RIAA to stop file-sharing[276] forward takedown notices to users without suspending their Internet service, [277] but it is unclear whether it will go further to aid the RIAA's initiatives. Similarly, in December 2009, Verizon announced that it would begin forwarding copyright infringement notices it receives from copyright holders[278] according to which, if Verizon receives multiple notices regarding alleged infringement, these users might "risk having their Internet service interrupted or turned off and [face] serious legal consequences if the copyright owner decides to sue over the alleged infringement."[279] On January 20, 2010, Verizon admitted that it had cut off service to a number of people who had been accused of sharing files. The Verizon spokesperson, Bobbi Henson, disclosed that Verizon had "cut some people off".[280]

In June 2008, Virgin Media began sending "educational" letters to thousands of Internet subscribers alleged to be file sharing illegally,[281] in a joint effort between Virgin Media and the British recording industry association, warned the recipients that file sharing would ultimately result in termination of their accounts.[282] Shortly afterward, it was announced that five more of Britain's largest Internet intermediaries had followed Virgin Media's lead and would begin their own «educational» letter campaigns.[283] In addition to threatening subscribers that illegal file sharing could lead to suspension or termination of Internet service, subscribers were warned that their online activities could be monitored and their Internet connection speeds could be degraded to make file sharing impractical.[284]

In May 2010, Eircom, the largest ISP in Ireland, announced that it would start cutting repeat accused copyright infringers off the Internet, appearing to be the first ISP in Europe to implement a voluntary "three-strikes" regime of graduated response.[285] This decision was the result of a settlement reached between IRMA (the Irish Recorded Music Association) and Eircom after a lawsuit filed by IRMA trying to hold EIRCOM liable for copyright violating users.[286] It is expected that, during the pilot phase, Eircom will process about 50 IP addresses a week.[287]

## Criticism

The three strikes approach has been widely critised. First it has been argued that the new graduated response plan is particularly troubling not only because it allows cut off Internet access to users without a trial, but also because the methods used to identify the users are notoriously faulty.[288] Professor Peter Yu cites several instances of internet users having been subjected to unverified suspicion of infringing activities through unreliable technologies including the case of a sick teenager who was sued for sharing ten songs via peer-to-peer networks when she was in hospital receiving weekly treatments for pancreatitis, and an 83-year-old deceased woman who did not use computers during her lifetime.[289]

Second many commentators consider that these laws will be difficult to enforce, that there will always exist a way to circumvent the laws and that only "occasional" (as opposed to persistent) pirates will be convinced by these laws to stop unlawful downloading. In any case, at this stage, no recommendation has yet been sent by HADOPI.[290] Moreover, in response to the graduate response scheme Pirate Bay[291] reminded internet users that its VPN is ready and willing to help them when they need it at a low fee.[292]

In addition, a new study carried out by the University of Rennes on the illegal downloading of online music and video in France revealed that it grew by three per cent between September and December 2009 - despite the passing of HADOPI law specifically designed to curb this practice.[293] It also concluded that

the suspension or permanent removal of an individual's Internet connection will be counterproductive as many who do pirate content also pay for items online as well.[294]

It also has to be noted that several jurisdictions, including Hong Kong, Germany, Spain, and Sweden have explicitly rejected the graduated response plans over concerns about the copyright holders' attempts to use the copyright laws to defend old business models and unknown implications.[295] In Australia in a recent court decision in a case involving the Australian Federation Against Copyright Theft (AFACT) against the Australian ISP iiNet, facilitating infringement of copyright it was determined that "the Court does not consider that warning and termination of subscriber accounts on the basis of AFACT Notices is a reasonable step, and further, that it would constitute a relevant power to prevent the infringements occurring [...][I]t would seem that termination of accounts in the circumstances of unproven and sporadic use, at least absent judicial consideration of the extent of the infringement on each account, would be unreasonable."[296]

On November 5, 2009 European Union lawmakers and Member State governments 5 agreed on safeguards against the suspension of Internet service to users merely suspected of copyright violations. The compromise agreement, contained in a telecommunications reform package, stated that restrictions on a user's internet access may only be taken "with due respect for the principle of presumption of innocence and the right to privacy."[297] There must be "a prior, fair and impartial procedure" guaranteeing "the right to be heard." Commissioner Reding said on this matter: "The new internet freedom provision represents a great victory for the rights and freedoms of European citizens [...] 'Three-strikes-laws', which could cut off Internet access without a prior fair and impartial procedure or without effective and timely judicial review, will certainly not become part of European law."[298] In addition, in April 2010 the European Commission welcomed the decision to make the draft of the Anti-Counterfeiting Trade Agreement (ACTA) available to the public clarifying that "no party in the ACTA negotiation is proposing that governments should introduce a compulsory "three strikes" or "gradual response" rule to fight copyright infringements and internet piracy."[299]

## Final remarks

It has been said that "the spread of information networks is forming a new nervous system for our planet."[300] It is also true that despite repressive regimes' attempts to suppress information, in many respects, information has never been so free. Information networks are finding a way to get through and allow people discover new facts thus making governments more accountable.[301] It is equally

true that it is rather unlikely to achieve an international consensus on freedom of speech on line and what that entails due to the highly diverse cultural, political, religious ethnical and social-economical backgrounds of the different countries around the world. On the other hand, most of the implementation of the censorship methods have been placed on private companies which are not always accountable as to their business dealings. It has become apparent that although private sector companies have a responsibility to respect and uphold the rights of customers and users, they cannot be expected to undertake on their own the task of resolving the political issues that threaten free expression on line.[302] His task requires a multi-sectoral approach and decisive legislative initiatives.

First there is the issue of corporate responsibility. Incidents involving major Western-based high-tech firms and the dealing with repressive regimes around the globe[303] have made clear that businesses, driven by the market opportunities for Internet services and equipment, have all engaged in various forms of self-censorship of their services and have been less than forthcoming about the specific compromises they make in order to do business in countries that engage in censorship and surveillance.[304] Forcing these private entities to take responsibility and leading them to include human rights risk assessments in their decisions about market entry and product development could only be achieved by both private initiatives and legislative measures. The Global Network Initiative (GNI) represents such an initiative encouraging the development of collaborative strategies bringing together businesses, industry associations, civil society organizations, investors and academics in an effort to create and implement a code of conduct for free expression and privacy in the ICT sector.[305] It is important that Internet giants Yahoo, Google and Microsoft launched the initiative, now encouraging and inviting other companies especially those in the ICT sector to join the effort.[306]

However, as mentioned above, private initiative alone is not enough. Legislative measures should also be adopted especially by countries who export this technology. These measures could include provisions for legal support for the victims, establishing disincentive for private corporations to collaborate with repressive surveillance and censorship, incentives for socially responsible technological development and measures to make collaboration with repression more difficult. The Global Online Freedom Act (GOFA)[307] aiming to prevent United States businesses from cooperating with repressive governments in Internet censorship and surveillance and to promote freedom of expression on the Internet would qualify as such a legislative piece. This bill was originally introduced in 2007, but it failed to gain traction in the U.S. House of Representatives. The bill was reintroduced in 2009.[308] GOFA would also create an Office of Global Internet Freedom at the State Department responsible for coordinating In-

ternet freedom efforts and conducting research.[309] Other private initiates on specific matter have also surfaced during the last years.[310]

Additional action needs to be taken on a multi-national global level. It has been argued that Internet censorship should be considered a barrier to trade under the World Trade Organization.[311] In November the European think tank ECIPE asserted that WTO member states are "legally obliged to permit an unrestricted supply of cross-border Internet services."[312]

The ongoing battle between copyright holders and the end users is also unlikely to stop. As a matter of fact, as outlined above, it appears to get more aggressive. The regulation of piracy on an individual level has become an arms race between the entertainment industries stringent regulations and the hackers who defy the rules.[313] Phil Shiller, Senior Vice President of Worldwide Product Marketing at Apple, Inc. has indicated that the solution is not the continuous technical development of technologies to restrict access, but rather one of behavioral education.[314] Over the past several years social and cultural norms shifted to accept the concept of P2P file sharing as acceptable.[315] It is established that there are two fundamental reasons P2P file sharers partake in this behavior: 1) they do not have to behave and 2) they do not want to. The initial stringent approach taken by RIAA's user-directed litigation campaign provided for a major public relations issue for music distributors after such cases as *Capital Records v. Thomas* and *BMG Music Entertainment v. Tenenbaum*.[316] Rather than finding a decrease in file sharing, after the thousands of cases prosecuted by the RIAA, surveys indicate that P2P participants increased. P2P members began to perfect closed networks and encrypted file transfers.[317]

What is transparent is the need to educate the public of laws protecting intellectual property. WIPO and the Copyright Society of the USA (CSUSA) are beginning to provide targeted educational materials to teenagers and children.[318] WIPO currently offers a 75-page book directed at "young students", which provides basic information about copyrights and challenges presented in the technical age.[319] On the CSUSA website there is a section called "Copyright Kids!" which also teaches children from fifth through eighth grade of US copyright laws.[320] Ultimately, the positive reinforcement of education may prove to be a stronger deterrent in the future than the penal system previously used by the entertainment industry.

Taking into account the challenges described above, it is clear that there is no single right answer to the issue of protecting the freedom of expression online. It is however equally clear that a policy aimed at supporting global Internet freedom requires a sophisticated, multi-faceted, multi-sectoral, and truly global approach

one that would bring together governments, companies and concerned citizens to find solutions to difficult new economic and security problems.

## Endnotes

1. *Reno v. ACLU*, 521 U.S. 844, 850-854 (U.S. 1997), where the Supreme Court provides an analysis of the Internet and its use. See also *Birth of the internet* providing a chronological map of the evolution of the Internet form the military network APRANET to today's web 0.2 available at http://www.cbc.ca/news/background/internet/(accessed May 27, 2010).
2. This term was populized through the 1990s to refer to digital communication systems and the internet telecommunications network and is associated with United States Senator and later Vice-President Al Gore. See also Gregory Gromov,"Roads and Crossroads of Internet History" at http://www.netvalley.com/cgi-bin/intval/net_history.pl (accessed June 6, 2010).
3. See Recommendations from the European Commission to the European Council: Europe and the Global Information Society (1994); First Annual Report of the Forum Information Society to the European Commission: Networks for People and their Communities. Making the Most of the Information Society in the European Union (1996); Resolution of the Council of Ministers, Nov. 21, 1996, 1996 O.J. (C 376) 1 (describing new policy-priorities regarding the information society); Interim Report from the High Level Expert Group on the Social and Societal Aspects of the Information Society: Building the European Information Society for Us All (1996). See also Al Gore, Bringing Information to the World: the Global Information Infrastructure, 9 Harv. J.L. & Tech. 1 (1996).
4. ACLU v. Reno, 929 F. Supp. 824, (E.D. Pa. 1996), aff'd, 521 U.S. 844 (1997).
5. Id. at 881. For an analysis of *ACLU v. Rend* in Greek See Bottis M., Censorship and minor protection - controllins access to internet "porn" material Human Rights, 31/2006, 849-894.
6. See infra Part III.
7. See http://www.internetworldstats.com/stats.htm.
8. A traditional definition is the one Madison states: that the ability to transmit information through one's own person (free speech) or through the use of other material property (free press) needs special protection from government interference. See John O. McGinnis, The Once and Future Property-Based Vision of the First Amendment, 63 U. Chi. L. Rev. 49, 56-57 (1996). Later, the concept was understood as being a social instrument in function of the democratic process: "The First Amendment does not protect a 'freedom to speak.' It protects the freedom of those activities of thought and communication by which we 'govern.'" Alexander Meiklejohn, The First Amendment is an Absolute, 1961 S. CT. Rev 245, 255. In Europe, the right to freedom of expression is interpreted as the right to seek, receive and impart information and ideas without interference by public authority and regardless of frontiers.
9. See John O. McGinnis, The Once and Future Property-Based Vision of the First Amendment, 63 U. Chi. L. Rev. 49, 19 (1996). As early as 1996 the author noted that at that time the press was the (only) medium for publishing thoughts to a wide audience, whereas today, computer networks are fast becoming the most cost-effective way of delivering information. Id. at 100.
10. Broadcasting was subjected to specific free speech rules. See generally Thomas G. Krattenmaker & Lucas A. Powe, Jr., Converging First Amendment Principles for Converging

Communications Media, 104 Yale L.J. 1719, 1721 (1995). See also Andreas Kohl, The International Aspects of the Freedom of Expression in Radio and Television, 8 Rev. Dr. H. 129 (1975); M. Bullinger Report on Freedom of Expression and Information: An Essential Element of Democracy, in Proceedings of the Sixth International Colloquy about the European Convention on Human Rights, 44, 86-126 (1985) available at: http://books.google.com/books?id=-3J_z-vs5qQC&pg=PA306&lpg=PA306&dq=Report+on+Freedom+of+Expression+and+Information:+An+Essential+Element+of+Democracy, +in+Proceedings+of+the+Sixth+International+Colloquy+about+the+European+Convention+on+Human+Rights&source=bl&ots=RheEY-Njyf&sig=cLQg_NyIzLKPot1obp-lA3EFHAM&hl=en&ei=s-X-S7qUM4_ANq20hTs&sa=X&oi=book_result&ct=result&resnum=1&ved=0CBMQ6AEwAA#v=onepage&q&f=false (accessed May 30, 2010).

11. "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances." Amendment 1 of the United States Constitution". The Bill of Rights: A Transcription. 8601 Adelphi Road, College Park, MD 20740-6001: The U.S. National Archives and Records Administration at: http://www.archives.gov/exhibits/charters/print_friendly.html?page=bill_of_rights_transcript_content.html&title=The%20Bill%20of%20Rights%3A%20A%20Transcription. (accessed June 17, 2010).

12. The first amendment applies to the executive branch [e.g., *Bernstein v. U.S. Dept. of State*, 974 F Supp 1288 (ND Cal 1997)[, and to the judicial branch [e.g., *Oregonian Pub. v. U.S. Dist. Court for Dist. of Or.*, 920 F2d 1462 (9th Cir 1990)]. The clause is fully applicable to state and local governments through the Due Process Clause of the Fourteenth Amendment. *Liquormart, Inc. v. Rhode Island*, 517 US 484, 116 S Ct 1495, 1501 n 1, 134 L Ed 2d 711 (1996).

13. The European Union is a political and economic transnational organisation of European countries, characterized by a distribution of lawmaking powers between the Union and the Member States. Its legislative branch is composed of the European Commission, the European Council of Ministers and the European Parliament. The European Court of Justice is responsible for interpreting EU law and for resolving disputes concerning the interpretation of Community Treaties. See generally P. Kent, Law of the European Union 10-88 (1996); P.S.R.F. Mathijsen, A Guide to European Union Law (1995) and Christopher Harding & Ann Sherlock, European Community Law (1995).

14. Koen Lenaerts, Fundamental Rights to be Included in a Community Catalogue, 16 Eur. L. Rev. 367, 371-372 (1991). This legal order has essentially a supervisory role, controlling the way in which member states comply with their ECHR obligations, but exercising no normative powers of its own. Id. See also Dirk Voorhoof, The Media in a Democratic Society, Legal Problems of the Functioning of Media in a Democratic Society 40-41 (Council of Europe ed. 1995) (describing the procedure in case of violation of the Convention by Member States). Still, the ECHR is a binding instrument for legislators of the Member States, as was explicitly confirmed in Article 1 of the Convention: "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention." Supervision of the application of the ECHR is the responsibility of the organs of the European Convention: the European Commission of Human Rights, the Committee of Ministers and the European Court of Human Rights. Id.

15. The European Commission of Human Rights at http://www.hri.org/docs/ECHR50.html#C.Art10 9ccessed June 15, 2010).
16. Caroline Uyttendaele & Joseph Dumortier, Free speech on the information superhighway: european perspectives, 16 J. Marshall J. Computer, &, Info. L. 905 (1998).
17. *Roth v. United States*, 354 U.S. 476 (1957) "whether to the average person, applying contemporary community standards, the dominant theme of the material, taken as a whole, appeals to the prurient interest." *Miller v. California*, 413 U.S. 15 (1973). Under the *Miller* test, a work is obscene if: (a)...'the average person, applying contemporary community standards' would find the work, as a whole, appeals to the prurient interest, ...(b)...the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law, and (c)...the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.
18. *Chaplinsky v. New Hampshire* (1942), "insulting or 'fighting words, ' those that by their very utterance inflict injury or tend to incite an immediate breach of the peace" are among the "well-defined and narrowly limited classes of speech [which] the prevention and punishment of...have never been thought to raise any constitutional problem."
19. *New York Times Co. v. Sullivan*.376 U.S. 254 (1964).
20. See for instance 17 U.S.C. § 512.
21. Caroline Uyttendaele & Joseph Dumortier, Free speech on the information superhighway: european perspectives, 16 J. Marshall J. Computer, &, Info. L. 905 (1998).
22. The European Commission of Human Rights at http://www.hri.org/docs/ECHR50.html#C.Art10 9ccessed June 15, 2010).
23. Caroline Uyttendaele & Joseph Dumortier, Free speech on the information superhighway: european perspectives, 16 J. Marshall J. Computer, &, Info. L. 905 (1998).
24. Jack M. Balkin, The Future of Free Expression in a Digital Age, 36 Pepp. L. Rev. 427, 434 (2009).
25. Jack M. Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79 N.Y.U.L. Rev. 1(2004).
26. Id.
27. Hannibal Travis, Opting Out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law, 84 Notre Dame L. Rev. 331 (2009).
28. Dawn C. Nunziato, The Death of the Public Forum in Cyberspace, 20 Berkeley Tech. L.J. 1115, 1122 (2005).
29. The term "Web 2.0" was coined by eminent technologist and writer Tim O'Reilly. See Tim O'Reilly, What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software, O'Reilly, Sept. 30, 2005, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.
30. Hannibal Travis, Opting Out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law, 84 Notre Dame L. Rev. 331 (2009).
31. Id.
32. Id.

33. Jack M. Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79 N.Y.U.L. Rev. 1(2004).
34. Id.
35. Id.
36. Id.
37. Id.
38. Id.
39. Secretary Clinton, January 2010, Remarks on Internet Freedom at http://www.state.gov/secretary/rm/2010/01/135519.htm (accessed June 15, 2010) "Because amid this unprecedented surge in connectivity, we must also recognize that these technologies are not an unmitigated blessing. These tools are also being exploited to undermine human progress and political rights. Just as steel can be used to build hospitals or machine guns, or nuclear power can either energize a city or destroy it, modern information networks and the technologies they support can be harnessed for good or for ill. The same networks that help organize movements for freedom also enable al-Qaida to spew hatred and incite violence against the innocent. And technologies with the potential to open up access to government and promote transparency can also be hijacked by governments to crush dissent and deny human rights."
40. Jack M. Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79 N.Y.U.L. Rev. 1(2004).
41. Hannibal Travis, Opting Out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law 84 Notre Dame L. Rev. 331 (2009).
42. Id. See also infra Part III & IV.
43. Lawrence Lessig & Paul Resnick. "Zoning Internet Speech," 98 *Michigan Law Review* 395 (1999).
44. Id. "For when viewed across jurisdictions, most controversial speech falls into category (3) - speech that is permitted to some in some places, but not to others in other places. What constitutes "political speech" in the United States (Nazi speech) is banned in Germany; what constitutes "obscene" speech in Tennessee is permitted in Holland; what constitutes porn in Japan is child porn in the United States; what is "harmful to minors" in Bavaria is Disney in New York".
45. T.G.I. Paris, May 22, 2000, Gaz. Pal. 2000, somm. jurispr. 1307. An English translation is available Yahoo! Case Tribunal De Grande Instance De Paris May 22, 2000, Juriscom.net, at http://juriscom.net/txt/jurisfr/cti/yauctions20000522.htm (last visited May 12, 2005).
46. Id.
47. Id.
48. Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme, 169 F. Supp. 2d 1181, 1186, 1194 (N.D. Cal. 2001).
49. Id. at 1193.
50. Id. However, a Ninth Circuit panel overturned the district court's decision because the district court improperly asserted personal jurisdiction over the French parties. 379 F.3d

1120 (9th Cir. 2004). The Ninth Circuit has granted en banc review of the case. 399 F.3d 1010 (9th Cir. 2005).

51. James Boyle, Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors, 66 U. Cin. L. Rev. 177 (1997).
52. Id.
53. For a short bio of John Gilmore see http://www.eff.org/about/board/ (accessed June 5, 2010).
54. Electronic Frontier Foundation (EFF), founded in 1990, is a non-profit organization dedicated to protecting defending free speech, privacy, innovation, and digital rights More information is vailable http://www.eff.org/about (accessed June 5, 2010).
55. James Boyle, Foucault in Cyberspace, 2 Yale Symp. L., &, Tech. 2 (2000): "This tenet contains a vital technical truth. The Internet is a distributed network. It is a system which has no central node, no organizing exchange-no one single radio tower, broadcasting device, or control center. Thus it is extremely hard to shut down the Net. You put a blockage in one place, and messages flow like water around it. In fact, "packet-switching" is basically a method of communication by hitchhiking. That is to say, when you write your e-mails or put together a web page, your data is broken up into several different packets, each carrying a little sign that says, "Going to New Haven." The packet of data then hitches a ride along the network. Some of the packets will travel by way of New York, some will travel by way of Boston, others will bounce around for ages until they finally get to their destinations where they will be integrated seamlessly. Try to imagine a censor trying to shut this thing down. It is like trying to grab the soap in the bath-you grab for it and it slips away. The idea of trying to exercise control over this seems impossible, hence the idea that the Internet treats censorship as a malfunction. The packets treat censorship the same way that they do a downed server-they just go around it."
56. Id.
57. Id.
58. Id. citing John P. Barlow's, Selling Wine Without Bottles: The Economy of Mind on the Global Net, article in which he credits Stewart Brand with the statement.
59. James Boyle, Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors, 66 U. Cin. L. Rev. 177, 182 (1997).
60. Id.
61. Id.
62. Id.
63. Reporters without Borders publish every year a list with the countries that regulate internet speech the most. This report is available at http://en.rsf.org/IMG/pdf/Internet_enemies.pdf (accessed May 25, 2010).
64. See, e.g., Pamela Samuelson, Intellectual Property Issues Raised by the National Information Infrastructure, 454 PLI/PAT 43 (1996).
65. See generally Lawrence Lessig Code version .2, John G. Palfrey, Jr. & Robert Rogoyski, The Move to the Middle: The Enduring Threat of "Harmful" Speech to Network Neutrality, 21 Wash. U. J.L. & Pol'y 31 (2006).

66. See Prt II above. See also Nicholas P. Dickerson, The thirteenth annual frankel lecture: comment: What makes the internet so special? And why, where, how, and by whom should its content be regulated?, 46 Hous. L. Rev. 61, 68-69 (2009).
67. Id.
68. Id.
69. See generally Lawrence Lessig, Code: Version 2.0, at 44-45 (2006) (explaining end-to-end theory).
70. See Lessig, supra note 37, at 44-45.
71. Id.
72. ACLU v. Reno (Reno I), 929 F. Supp. 824, 883 (E.D. Pa. 1996) (Dalzell, J., concurring).
73. See John G. Palfrey, Jr. & Robert Rogoyski, The Move to the Middle: The Enduring Threat of "Harmful" Speech to the End-to-End Principle, 21 Wash. U. J.L. & Pol'y 31, 36-37 (2006).
74. See generally Jonathan Zittrain, Internet Points of Control, 44 B.C. L. Rev. 659 (2003).
75. Id.
76. 47 U.S.C. §223 (2000).
77. 15 U.S.C. §7701 (2000); see also Derek E. Bambauer, Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-mail Advertising, 10 Va. J.L. & Tech. 5 (2005).
78. See Jonathan Zittrain, Internet Points of Control, 44 B.C. L. Rev. 659, 671-672 (2003).
79. Michael Geist, "The music industry's digital reversal," The Toronto Star, January 12, 2009. Available at: http://www.thestar.com/sciencetech/article/569203 (accessed May 28, 2010).
80. 579 F. Supp. 2d 1210 (D. Minn. 2008).
81. See Thomas, 579 F. Supp. 2d at 1226-27. The jury in the first trial returned a verdict against Thomas and awarded the plaintiffs statutory damages of $ 222, 000 to compensate for twenty-four downloaded songs. The case was subsequently retried. In his decision granting Thomas's motion for a new trial based on an erroneous jury instruction, the judge himself said he thought the damages awarded were excessive, and he implored Congress to revisit the criteria for awarding large statutory damages in cases involving noncommercial infringement by individual consumers. See also Richard Koman, Wow! Jury Verdict in *Capitol v. Thomas-Rasset:* $ 2 Million, ZDNET, June 18, 2009, http://government.zdnet.com/?p=4990. Thomas's motion for a retrial was granted based on an error in the judge's jury instructions concerning whether the "making available" of music for download qualifies as distribution within the meaning of the Copyright Act.
82. Capitol Records Inc. v. Thomas-Rasset, No. 06-1497 (MJD/RLE), 2010 U.S. Dist. LEXIS 504, at 1 (D. Minn. Jan. 22, 2010). at 2.
83. see Tenenbaum, 2009 U.S. Dist. LEXIS 112845, at 2-3; see also 17 U.S.C. § 107 (2006).
84. Student Ordered to Pay $ 675k for Downloads, CBS News, July 31, 2009, http://www.cbsnews.com/stories/2009/07/31/tech/main5203118.shtm (accessed June 6, 2010).

85. David Kravets, Judge Finalizes $ 675, 000 RIAA Piracy Verdict, Won't Gag Defendant, Wired, Dec. 7, 2009, http://www.wired.com/threatlevel/2009/12/piracy-verdict-finalized (accessed June 6, 2010).
86. Genan Zilkha, The RIAA's Troubling Solution to File-Sharing, 20 Fordham Intell. Prop. Media, &, Ent. L.J. 667 (2010) Part I.B.
87. Sarah McBride and Ethan Smith, "Music Industry to Abandon Mass Suits," The Wall Street Journal, December 19, 2008. Available at: http://online.wsj.com/article/SB122966038836021137.html.
88. Mary Madden, Senior Research Specialist, The State of Music Online: Ten Years After Napster, Pew Internet & American Life Project, June 2009, pp 10-13. (accessed June 6, 2010).
89. Sarah McBride and Ethan Smith, "Music Industry to Abandon Mass Suits," The Wall Street Journal, December 19, 2008. Available at: http://online.wsj.com/article/SB122966038836021137.html (accessed June 6, 2010).
90. 15 U.S.C. §§7704-05 (2000).
91. Id. §§6501-06.
92. See OpenNet Initiative, Global Internet Filtering Map, http://map.opennet.net/ (identifying countries that partake in filtering on the internet);see also Reporters Sans Frontières - Web 2.0 versus Control 2.0 available at http://en.rsf.org/web-2-0-versus-control-2-0-18-03-2010, 36697 (accessed June 6, 2010).; also Internet enemies and countries under surveillance at http://en.rsf.org/IMG/pdf/Internet_enemies.pdf (accessed June 6, 2010).
93. John G. Palfrey, Jr. & Robert Rogoyski, The Move to the Middle: The Enduring Threat of "Harmful" Speech to Network Neutrality, 21 Wash. U. J.L. & Pol'y 31 (2006).at 36-37 (noting the "tension between the desirability of the end-to-end principle and the desire to regulate certain behavior online").
94. Need more citations re regulation of intermediaries Kathleen M. Sullivan & Gerald Gunther, Constitutional Law 1501 (15th ed. 2004).
95. See Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 405 (2008).
96. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.); 47 U.S.C. § 230(c)(1) (2000).
97. See, e.g., Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997) (finding AOL not liable for defamatory statements published by one of its users); see also Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003) (holding GTE not liable after a user of one of its websites posted illegal videos of athletes changing in their locker room).
98. 17 U.S.C. § 512(c)(1)(A)(iii) (2004).
99. See 17 U.S.C. § 512(a) (2006); § 512. Limitations on liability relating to material online (a) Transitory digital network communications. A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if- (1) the

transmission of the material was initiated by or at the direction of a person other than the service provider; (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider; (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person; (4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and (5) the material is transmitted through the system or network without modification of its content and injunctive relief against them must be limited to a court order requiring the termination of the Internet access of a subscriber or account holder adjudged to have engaged in infringing activity, or reasonable steps to block access from within the United States to a specific online location outside the United States adjudged to be infringing See id. id. § 512(j)(1)(B);

100. Council Directive 2000/31, 2000 O.J. (L 178) 1 [hereinafter ECD].

101. See id. art. 12, at 12.

102. Id. art. 14, at 13.

103. John G. Palfrey, Jr. & Robert Rogoyski, The Move to the Middle: The Enduring Threat of "Harmful" Speech to Network Neutrality, 21 Wash. U. J.L. & Pol'y 31 (2006). at 31. See also generally Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, (2008).

104. The Middle East and North Africa is one of the most heavily censored regions in the world.

105. See genrally Code.2 http://en.rsf.org/IMG/pdf/Internet_enemies.pdf; also The thirteenth annual frankel lecture: comment: what makes the internet so special? And why, where, how, and by whom should its content be regulated?, 46 Hous. L. Rev. 61 (2009).

106. Testimony of Rebecca MacKinnon, Visiting Fellow, Center for Information Technology Policy, Princeton University Co-Founder, Global Voices Online (globalvoicesonline.org) http://www.internationalrelations.house.gov/111/mac031010.pdf (accessed May 25, 2010).

107. For more details on these filtering techniques, see Steven J. Murdoch and Ross Anderson, "Tools and Technology of Internet Filtering," Access Denied, (Cambridge: MIT Press, 2008), available at: http://opennet.net/sites/opennet.net/files/Deibert_04_Ch03_057-072.pdf . See also the OpenNet Initiative, "About Filtering," http://opennet.net/about-filtering (accessed May 25, 2010).

108. Id.

109. Id. See also *United States v. Am. Library Ass'n,* 539 U.S. 194 (U.S. 2003) (Stevens, J., dissenting: "Because of this "underblocking," the statute will provide parents with a false sense of security without really solving the problem that motivated its enactment. Conversely, the software's reliance on words to identify undesirable sites necessarily results in the blocking of thousands of pages that "contain content that is completely innocuous for both adults and minors, and that no rational person could conclude matches the filtering companies' category definitions, such as 'pornography' or 'sex.'" Id., at 449. In

my judgment, a statutory blunderbuss that mandates this vast amount of "overblocking" abridges the freedom of speech protected by the First Amendment).

110. OpenNet Initiative, "About Filtering," http://opennet.net/about-filtering (accessed May 25, 2010). "Filtering based on dynamic content analysis—effectively reading the content of requested websites—though theoretically possible, has not been observed in our research".

111. Id.

112. Nart Villeneuve, The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace, First Monday, Jan. 4, 2006, http://firstmonday.org/issues/issue11 1/villeneuve/index.html.

113. Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008) citing Nart Villeneuve, The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace, First Monday, Jan. 4, 2006, http://firstmonday.org/issues/issue11 1/villeneuve/index.html (accessed June 6, 2010).

114. Id.

115. Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).

116. See Jonathan Zittrain, Internet Points of Control, 44 B.C. L. Rev. 653 (2003).

117. Testimony of Rebecca MacKinnon Visiting Fellow, Center for Information Technology Policy, Princeton University Co-Founder, Global Voices Online (globalvoicesonline.org) http://www.internationalrelations.house.gov/111/mac031010.pdf (accessed June 6, 2010).

118. See http://opennet.net/research/profiles/china#footnote6_tic8bin (accessed June 6, 2010).

119. Google INC presents to users a clear notification whenever links have been removed from our search results in response to local laws and regulations in China.2 – Google available at: Schrage, E. (2006). "Testimony of Google Inc." Joint Hearing of the Subcommittee on Africa, Global Human Rights & International Operations and the Subcommittee on Asia and the Pacific. Retrieved, May 22 2008, from http://googleblog.blogspot.com/2006/02/testimony-internet-in-china.html (accessed June 6, 2010).

    Where a government requests that we restrict search results, we will do so if required by applicable law and only in a way that impacts the results as narrowly as possible. If we are required to restrict search results, we will strive to achieve maximum transparency to the user. - Yahoo! available at: Callahan, Michael. (2006). "Testimony of Michael Callahan." Joint Hearing of the Subcommittee on Africa, Global Human Rights & International Operations and the Subcommittee on Asia and the Pacific. Retrieved, May 22 2008, from http://yhoo.client.shareholder.com/releasedetail.cfm?releaseid=187725.

    When local laws require the company to block access to certain content, Microsoft will ensure that users know why that content was blocked, by notifying them that access has been limited due to a government restriction. – Microsoft available at: Krumholtz, J. (2006). "Congressional Testimony: The Internet in China: A Tool for Freedom or Suppression?" Joint Hearing of the Subcommittee on Africa, Global Human Rights & International Operations and the Subcommittee on Asia and the Pacific. Retrieved,

May 22 2008, from http://www.microsoft.com/presspass/exec/krumholtz/02-15WrittenTestimony.mspx.

120. Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).
121. Ronald Deibert, China's Cyberspace Control Strategy, February 2010, available at http://www.onlinecic.org/resourcece/archives/chinapapers (accessed June 5, 2010).
122. Nart Villeneuve, Search Monitor Project: Toward a Measure of Transparency, 2008, http://www.nartv.org/projects/search_monitor/searchmonitor.pdf (accessed June 6, 2010).
123. Id.
124. Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).
125. The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs, at the University of Toronto, Canada focusing on advanced research and development at the intersection of digital media, global security, and human rights, http://citizenlab.org/ (accessed June 5, 2010).
126. Nart Villeneuve, Search Monitor Project: Toward a Measure of Transparency, 2008, http://www.nartv.org/projects/search_monitor/searchmonitor.pdf; also Ronald Deibert, China's Cyberspace Control Strategy, February 2010, available at *http://www.onlinecic.org/resourcece/archives/chinapapers* (accessed June 5, 2010).
127. Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008) citing Ronald Deibert, The Geopolitics of Asian Cyberspace, Far E. Econ. Rev., Dec. 2006, http://www.feer.com/articles1/2006/0612/free/p022.html.
128. Google and the threat to free speech - Times Online, available at: http://technology.timesonline.co.uk/tol/news/tech_and_web/article3634123.ece.
129. A new approach to China http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.
130. A new approach to China http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.
131. Id. See also Google to Stop Censoring Search Results in China After Hack Attack, Kim Zetter, available at: http://www.wired.com/threatlevel/2010/01/google-censorship-china/#ixzz0qvKA5zOI (accessed June 6, 2010).
132. A new approach to China: an update, 3/22/2010 available at: http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html.
133. Nart Villeneuve, March 23, 2010 http://www.nartv.org/2010/03/23/google-cn-google-com-hk/.
134. Id.
135. Lawrence Lessig, Code Version 2.0, at 39 (2006).
136. OpenNet Initiative, A Starting Point: Legal Implications of Internet Filtering 5 (Sept. 2004), available at http://opennet.net/docs/Legal Implications.pdf.
137. Bernhard Warner, Google and the threat to free speech - Times Online March 27, 2008 available at: http://technology.timesonline.co.uk/tol/news/tech_and_web/article3634123.ece (accessed

May 20, 2010); See also sami ben gharbia, Free Speech Roundup: Indonesia, Saudi Arabia, Turkey, Yemen available at:

http://globalvoicesonline.org/2008/04/05/free-speech-roundup-indonesia-saudi-arabia-turkey-yemen/(accessed May 20, 2010).

138. Sami Ben Gharbia, Free Speech Roundup: Indonesia, Saudi Arabia, Turkey, Yemen available at: http://globalvoicesonline.org/2008/04/05/free-speech-roundup-indonesia-saudi-arabia-turkey-yemen/(accessed May 20, 2010).

139. Bernhard Warner, Google and the threat to free speech - Times Online March 27, 2008 available at: http://technology.timesonline.co.uk/tol/news/tech_and_web/article3634123.ece (accessed May 20, 2010).

140. Id.

141. *Babar Dogar, Associated Press, Pakistan lifts Facebook ban - Yahoo! News, May 31, 2010 available at* http://news.yahoo.com/s/ap/20100531/ap_on_re_as/as_pakistan_internet_crackdown (accessed June 5, 2010).

142. Id. See also Facebook apologizes to Pakistan over 'sacrilegious' content available at http://www.siasat.pk/forum/showthread.php?36763-Facebook-Apologizes-to-Pakistan-IT-Ministry-Official&p=181185 (accessed June 6, 2010).

143. Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 412 (2008).

144. See Human Rights in China, HRIC Case Highlight: Shi Tao and Yahoo, http://www.hrichina.org/public/highlight (summarizing Shi Tao's case) (accessed June 3, 2010); also Human Rights USA at http://www.humanrightsusa.org/index.php?option=com_content&task=view&id=15&Itemid=35 (accessed June 5, 2010).

145. *Changsha People's Procuratorate of Hunan Province v. Shi Tao* (Changsha Interm. People's Ct. of Hunan Province, Apr. 27, 2005), translated in Case No. 19-10, at 29, http://www.globalvoicesonline.org/wp-content/ShiTao verdict.pdf In the judgment, it was revealed that Shi used his anonymous personal email account of huoyan-1989@yahoo.com.cn to send the notes. He identified himself as "198964." Id. at 29.

146. Changsha People's Procuratorate of Hunan Province v. Shi Tao (Changsha Interm. People's Ct. of Hunan Province, Apr. 27, 2005), translated in Case No. 19-10, at 29, http://www.globalvoicesonline.org/wp-content/ShiTao verdict.pdf(accessed June 6, 2010).

147. *Changsha People's Procuratorate of Hunan Province v. Shi Tao,* supra note 145 at 31.

148. Id. at 28-29.

149. Id. at 32.

150. The Internet in China: A Tool for Freedom or Suppression?: Joint Hearing Before the Subcomm. on Africa, Global Human Rights and International Operations and the Subcomm. on Asia and the Pacific of the Comm. on International Relations, 109th Cong. 55, 58-59 (2006) [hereinafter Joint Hearing on the Internet in China] (statement of Michael Callahan, Senior Vice President and General Counsel, Yahoo! Inc.), available at http://www.foreignaffairs.house.gov/archives/ 109/26075.pdf(accessed June 6, 2010).

151. See also Statement of Chairman Lantos at hearing, Yahoo! Inc.'s Provision of False Information to Congress". http://www.internationalrelations.house.gov/press_display.asp?id=446 (accessed June 6, 2010).

152. Testimony of Michael Callahan, Senior Vice President and General Counsel, Yahoo! Inc., Before the Subcommittees on Africa, Global Human Rights and International Operations, and Asia and the Pacific," U.S. House of Representatives Committee on International Relations, Joint Hearing: "The Internet in China: A Tool for Freedom or Suppression?" February 15, 2006, online at: http://www.nytimes.com/packages/pdf/business/YahooStatement.pdf (accessed June 6, 2010).

153. Reporters Without Borders, Verdict in Cyberdissident Li Zhi Case Confirms Implication of Yahoo!, Feb. 27, 2006, http://www.rsf.org/article.php3?id article=16579 (accessed June 6, 2010). See also http://www.humanrightsusa.org/index.php?option=com_content&task=view&id=15&Itemid=35.

154. Reporters Without Borders, Verdict in Cyberdissident Li Zhi Case Confirms Implication of Yahoo!, Feb. 27, 2006, http://www.rsf.org/article.php3?id article=16579. A Chinese version of the judgment is available at http://www.rsf.org/IMG/pdf/li zhi verdict.pdf. (accessed June 6, 2010).

155. Shi Tao, Yahoo!, and the lessons for corporate social responsibility, Rebecca MacKinnon, online at http://rconversation.blogs.com/YahooShiTaoLessons.pdf (accessed June 6, 2010).

156. Second Amended Complaint for Tort Damages at 14, Wang Xiaoning v. Yahoo! Inc., No. C07-02151 CW (N.D. Cal. July 30, 2007). The deprivation of political rights in China involves a fixed period of time after an individual is released from prison during which he or she is denied the rights of free speech and association granted to other citizens. U.S. Dep't of state, bureau of democracy, human rights, and labor, china: country reports on human rights practices 2007 (2008), *available at* http://www.state.gov/g/drl/rls/hrrpt/2007/100518.htm (accessed June 6, 2010).

157. Joint Stipulation of Dismissal at 1, *Wang Xiaoning v. Yahoo! Inc.,* No. C07- 02151 CW/JCS (N.D. Cal. Nov. 13, 2007). (accessed June 6, 2010).

158. Seth Frinkelstein, Do You Have any Idea Who Last Looked at Your Data?, Guardian.co.uk, Nov. 15, 2007, http://www.guardian.co.uk/technology/2007/nov/15/comment. (accessed June 6, 2010).

159. Jacqui Chen, Maybe a little evil: Google outs Indian man to authorities, at http://arstechnica.com/tech-policy/news/2008/05/maybe-a-little-evil-google-outs-indian-man-to-authorities.ars: see also Google and India Test the Limits of Liberty, Amol Sharma and Jessica E. Vascellaro at http://online.wsj.com/article/SB126239086161213013.html (accessed June 6, 2010).

160. Id.

161. Google Defends Helping Police Nab Defamer, By John Ribeiro, IDG News, http://www.pcworld.com/businesscenter/article/146049/google_defends_helping_police_nab_defamer.html (accessed June 16, 2010).

162. Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 2006 U.S. Dist. LEXIS 49955 (N.D. Cal. 2006) Electronic Frontier Found., EFF's Case Against AT&T at http://www.eff.org/nsa/hepting (accessed June 5, 2010).

163. Id.

164. See *Gonzales v. Google, Inc.*, 234 F.R.D. 674, 688 (N.D. Cal. 2006).

165. Id. At 679.

166. Christopher Soghoian, 8 Million Reasons for Real Surveillance Oversight, December 1, 2009, at://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html (accessed June 14, 2010); also Kim Zetter, Yahoo Issues Takedown Notice for Spying Price List, December 4, 2009 at http://www.wired.com/threatlevel/2009/12/yahoo-spy-prices/#ixzz0rDmlsB6l (accessed June 14, 2010).

167. Id.

168. Id. "I theorized that if I could obtain the price lists of each ISP, detailing the price for each kind of service, and invoices paid by the various parts of the Federal government, then I might be able to reverse engineer some approximate statistics."

169. Id. Also http://files.cloudprivacy.net/verizon-price-list-letter.PDF (accessed June 20, 2010).

170. See also http://files.cloudprivacy.net/yahoo-price-list-letter.PDF(accessed June 20, 2010).

171. Available at http://www.google.com/governmentrequests/).

172. Greater transparency around government requests David Drummond, SVP, Corporate Development and Chief Legal Officer at http://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html (accessed June 16, 2010).

173. See Government requests http://www.google.com/governmentrequests/faq.html.

174. Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).

175. Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).

176. Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).

177. Id.

178. Id.

179. Anne Chueng & Rolf H. Weber, Internet Governance and the Responsibility of Internet Service Providers, 26 Wis. Int'l L.J. 403, 411 (2008).

180. Jennifer A. Chandler, A Right to Reach an Audience: An Approach to Intermediary Bias on the Internet, 35 Hofstra L. Rev. 1095, 1117 (2007).

181. Search Engine Use, Data Memo by Deborah Fallows, Senior Research Fellow, Pew Internet and American Life Project, August 6, 2008. At http://www.pewinternet.org/PPF/r/258/report_display.asp (accessed June 15, 2010).

182. http://en-us.nielsen.com/rankings/insights/rankings/internet; see also http://marketshare.hitslink.com/search-engine-market-share.aspx?qprid=5.

183. Jennifer A. Chandler, A Right to Reach an Audience: An Approach to Intermediary Bias on the Internet, 35 Hofstra L. Rev. 1095, 1117 (2007) discussing Google's decision to remove the websites of BMW Germany and Ricoh Germany from its index because they had used

banned methods to manipulate the search engine as well as the case of *Search King, Inc. v. Google Technology, Inc.* which dealt with a dispute over Google's ranking demotion of the plaintiff's website. Search King offered a match-making service designed to assist clients to buy and sell links from highly ranked websites in the hope of increasing the ranking of the linked-to websites. Google admitted that it had deliberately decreased the ranking of the Search King websites, stating that it was entitled to do so because Search King's actions undermined the integrity of its PageRank system while Search King argued that Google had demoted its websites because it was competing with Google, and sued for tortious interference with contractual relations. *In Langdon v. Google, Inc.* 2007 WL 530156 CD.Del. Feb. 20, 2007, the plaintiff complained that Google would not let him purchase ads to advertise his websites, which criticized the North Carolina Attorney General (www.ncjusticefraud.com) and the Chinese government (www.chinaisevil.com). Google refused his anti-North Carolina Attorney General ad, citing its policy against advertisements that "advocate against an individual, group or organization" but failed to issue any decision regarding the plaintiff's short anti-China advertisement.

184. See Andrew Goodman, Search Engine Showdown: Black Hats v. White Hats at SES, SearchEngineWatch, Feb. 17, 2005, http://searchenginewatch.com/showPage.html?-page=3483941. (accessed June 15, 2010).

185. Google writes: "Links help our crawlers find your site and can give your site greater visibility in our search results." Google Webmaster Help Center, How Can I Create a Google-friendly Site?, www.google.com/support/webmasters/bin/answer.py?answer=40349&topic=8522 (last visited Mar. 3, 2007).

186. Google informs webmasters that "Google counts the number of votes a page receives as part of its PageRank assessment, interpreting a link from page A to page B as a vote by page A for page B. Votes cast by pages that are themselves "important' weigh more heavily and help to make other pages "important.'" Id.

187. Eric Goldman, Search Engine Bias and the Demise of Search Engine Utopianism, 8 Yale J.L. & Tech. 188, 189 (2006) (noting that search engines wield "significant power to shape searcher behavior and perceptions ... [and] the choices that search engines make about how to collect and present data can have significant social implications").

188. Jennifer A. Chandler, A Right to Reach an Audience: an Approach to Intermediary Bias on the Internet, 35 Hofstra L. Rev. 1095 1117 (2007).

189. A selection of recent papers includes Urs Gasser, Regulating Search Engines: Taking Stock and Looking Ahead, 8 Yale J.L. & Tech. 201, 208-16 (2006). (advocating a complete assessment of alternative regulatory approaches prior to deciding legislative intervention is the best solution); Goldman, supra note 45 (arguing that search engine bias is necessary and desirable, and that regulatory intervention is unwarranted); Frank Pasquale, Rankings, Reductionism, and Responsibility, 54 Clev. St. L. Rev. 115, 135-39 (2006) (proposing legal remedies for harms claimed to flow from unwanted inclusion or exclusion in search engine results); Andrew Sinclair, Note, Regulation of Paid Listings in Internet Search Engines: A Proposal for FTC Action, 10 B.U. J. Sci. & Tech. L. 353, 364-66 (2004) (advocating, among other things, FTC action against search engines that use paid listings without disclosing this fact to consumers).

190. Introna & Nissenbaum, supra note 7, at 61; Gasser, supra note 41, at 232-34.

191. Gasser, supra note 189 at 233.
192. Gasser, supra note 189, at 233-34.
193. America Online, Agreement to Rules of User Conduct, at http://www.aol.com/copyright/rules.html (accessed June 15, 2010).
194. Id.
195. Yahoo!, Terms of Service, at http://docs.yahoo.com/info/terms (accessed June 15, 2010).
196. Id. Dawn Nunziato The Death of the Public Forum in Cyberspace, 20 Berkeley Tech. L.J. 1115 (2005).
197. Comcast Cable Communications, LLC, Comcast High-Speed Internet Acceptable Use Policy, at http://www.comcast.net/terms/use.jsp (accessed June 15, 2010).
198. Dawn Nunziato, The Death of the Public Forum in Cyberspace, 20 Berkeley Tech. L.J. 1115 (2005)1120-1123. The author also discusses how Colleges and universities, both private and public, also serve as Internet access providers for millions of students across the United States have established and enforced "acceptable use policies" that substantially restrict First Amendment protected speech.aas well as private employers, which serve as Internet access providers for millions of employees across the United States, routinely monitor and restrict e-mail (and Internet use generally), with approximately 50-60% of employers monitoring e-mail.
199. Chris Sogohian, Google censors political-donation transparency ads, December 17, 2008 at http://news.cnet.com/8301-13739_3-10122713-46.html (accessed June 10, 2010).
200. Id.
201. Sherriff, Lucy (21 September 2006). "Google erases Operation Ore campaign site". The Register. http://www.theregister.co.uk/2006/09/21/google_delists_inq21/. (accessed June 15, 2010).
202. Christopher Landau Google climbdown on abortion ads, 17 September 2008 http://news.bbc.co.uk/2/hi/uk_news/7621751.stm (accessed June 15, 2010).
203. Dawn Nunziato The Death of the Public Forum in Cyberspace, 20 Berkeley Tech. L.J. 1115, 1124-1125 (2005).
204. Id. at n.28.
205. Barbara van Schewick, Towards an Economic Framework for Network Neutrality Regulation, 5 J. Telecomm. & High Tech. L. 329, 336 (2007).
206. Benjamin Rupert, The 110th Congress and Network Neutrality: S. 215 - The Internet Freedom Preservation Act, 18 DePaul J. Art, Tech. & Int'l Intell. Prop. L. 325, 240-41 (2008).
207. Dawn Nunziato, The Death of the Public Forum in Cyberspace, 20 Berkeley Tech. L.J. 1115, 1123 (2005)
208. Don Marti, "Google Begins Making DMCA Takedowns Public," Linux Journal (2002/4/12) (describing Google's response to the Scientologists and subsequent decision to contribute to ChillingEffects.org). Gallagher, David F. (2002-04-22) http://www.linuxjournal.com/article/5997 (accessed June 15, 2010); "New Economy; A copyright dispute with the Church of Scientology is forcing Google to do some creative linking". New York Times.

http://query.nytimes.com/gst/fullpage.html?res=9F02E5D7103FF931A15757C0A9649C8B63&sec=&spon=&pagewanted=all (accessed May 29, 2010).

209. "Google Somewhat Lifts Oceana Ad Ban". webpronews.com. 2004-05-17(accessed June 10, 2010). http://www.webpronews.com/topnews/2004/05/17/google-somewhat-lifts-oceana-ad-ban.The policy was later changed.

210. See Brian Stelter, To Curb Traffic on the Internet, Access Providers Consider Charging by the Gigabyte, N.Y. Times, June 15, 2008, at A1, available at http://www.nytimes.com/2008/06/15/technology/15cable.html?pagewanted=1 (accessed June 15, 2010).

211. Id.

212. EFF Test Your ISP https://www.eff.org/testyourisp (accessed June 15, 2010).: "In specific, Comcast was injecting forged RST packets into TCP communications, in an effort to disrupt certain protocols commonly used for file-sharing. The interference efforts were triggered by the protocol that the subscriber used, not by the number of connections made or amount of bandwidth used by the subscriber".

213. Peter Eckersley, Fred von Lohmann and Seth Schoen November 28, 2007http://www.eff.org/files/eff_comcast_report2.pdf(accessed June 15, 2010).; see also In re Free Press & Pub. Knowledge, 23 F.C.C.R. 13028, 13031 (2008) (describing the AP study). Comcast argued that it was merely slowing and not actually blocking P2P traffic, but the Federal Communications Commission found otherwise. See id. at 13053-54 (finding that "whether or not blocking was Comcast's intent, Comcast's actions certainly had that effect in some circumstances").

214. Comcast Corp. v FCC, No. 08-1291 (D.C. Cir., Apr. 6, 2010) Full text of opinion available at: http://pacer.cadc.uscourts.gov/common/opinions/201004/08-1291-1238302.pdf (accessed June 15, 2010).

215. Tyler Lacey April 11, 2010 Comcast Corp. v. FCC D.C. Circuit Denies FCC Jurisdiction to Mandate Net Neutrality http://jolt.law.harvard.edu/digest/telecommunications/comcast-corp-v-fcc; also Stacey Higginbotham, Comcast vs FCC: In Battle For Net Neutrality, Did the Courts Hand Comcast a Pyrrhic Victory? April 6, 2010 at: http://gigaom.com/2010/04/06/did-the-courts-hand-comcast-a-pyrrhic-victory/(accessed June 15, 2010).

216. Bloomberg Businessweek, Comcast Wins in Case on FCC Net Neutrality Powers (update 6) http://www.businessweek.com/news/2010-04-06/comcast-wins-in-case-on-fcc-net-neutrality-powers-update6-.html (June 4, 2010)

217. Paul Barbagallo, FCC Broadband Proposal Faces New Scrutiny, With Over 240 House Members Now Opposed, June 2, 2010 http://news.bna.com/pwdm/PWDMWB/split_display.adp?fedfid=17261986&vname=prabulallissues&wsn=499750500&searchid=11543456&doctypeid=1&type=date&mode=doc&split=0&scm=PWDMWB&pg=0 (subscription required) (accessed June 15, 2010).; also *Fred von Lohmann,* Court Rejects FCC Authority Over the Internet, April 6, 2010, at: https://www.eff.org/deeplinks/2010/04/court-rejects-fcc-authority-over-internet (accessed June 15, 2010).

218. Brett M. Frischmann & Barbara van Schewick, Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo, 47 Jurimetrics J. 383, 387-89 (2007). See also Milton Mueller Net Neutrality as Global Norm for Internet Governance at http://www.internetgovernance.org/pdf/NetNeutralityGlobalPrinciple.pdf (accessed June 15, 2010).

219. See Lawrence Lessig, The Future of Ideas, 2002, 46-48, 155-76, 246-49.

220. See, also Adam Liptak, Verizon Rejects Text Messages from an Abortion Rights Group, N.Y. Times, Sept. 27, 2007, at A1 (citation omitted); Adam Liptak, Verizon Reverses Itself on Abortion Messages, N.Y. Times, Sept. 28, 2007, available at http://www.nytimes.com/2007/09/28/business/28verizon.html (accessed June 15, 2010).

221. Jack M. Balkin, Free speech and press in the digital age: the future of free expression in a digital age, 36 Pepp. L. Rev. 427, 444 (2009).

222. Barbara van Schewick, Towards an Economic Framework for Network Neutrality Regulation, 5 J. Telecomm. & High Tech. L. 329, 336 (2007).

223. See Peter Svensson, Comcast Blocks Some Internet Traffic, S.F. Chron., Oct. 19, 2007, available at http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2007/10/19/financial/f061526D54.DTL&feed=rss.business. (accessed June 15, 2010).

224. Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme, 169 F. Supp. 2d 1181, 1186, 1194 (N.D. Cal. 2001).

225. See Lori Enos, Yahoo! To Ban Nazi-Related Auctions, E-Commerce Times, Jan. 3, 2001, available at http://www.ecommencetimes.com/story/6432.html (accessed June 15, 2010).

226. Alexander Tsesis, Hate in Cyberspace: Regulating Hate Speech on the Internet, 38 San Diego L. Rev. 817, 866 (2001).

227. Dawn Nunziato The Death of the Public Forum in Cyberspace, 20 Berkeley Tech. L.J. 1115 (2005).

228. Jack M. Balkin, Free speech and press in the digital age: the future of free expression in a digital age, 36 Pepp. L. Rev. 427 (2009).

229. Jack M. Balkin, The Future of Free Expression in a Digital Age, 36 Pepp. L. Rev. 16 (2009).

230. See above Part II.

231. 17 U.S.C. 512(h). Doris E. Long, Electronic voting rights and the dmca: another blast from the digital pirates or a final wake up call for reform?" 23 J. Marshall J. Computer & Info. L. 533, 535-540.

232. Id. "To obtain the subpoena, the copyright owner is only required to provide a written notice that includes the following: (1) a clear identification of the copyrighted work allegedly being infringed; (2) a clear identification of the alleged infringing material; (3) "reasonably sufficient" information that will allow the ISP to locate the material at issue; (4) a statement of good faith belief the work is being infringed; and (5) a declaration that the identity of the subscriber in question will only be used for the purpose of protecting the owner's copyright."

233. 17 U.S.C. 512(c).

234. 17 U.S.C. 512(h)(5).

235. Id.

236. *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Service.*, 351 F.3d 1229 (D.C. Cir. 2003).

237. See id. at 1237.

238. see also John Borland, Court: RIAA Lawsuit Strategy Illegal, CNET News, Dec. 19, 2003, http://news.cnet.com/2100-1027_3-5129687.html [hereinafter Borland, RIAA Lawsuit]. Before the Verizon decision came down, the RIAA had already issued more than 3, 000 subpoenas. Electronic Frontier Found., RIAA v. The People: Four Years Later 5 (2007), available at http://w2.eff.org/IP/P2P/riaa_at_four.pdf. Users who received this subpoena included a twelve-year-old girl living in a housing project in New York City, and a grandmother, whom, it was later discovered, had been wrongfully accused. Id. at 4. The accused were given the opportunity to settle or go to trial. Id. The majority of users settled for around $ 3, 000. Id. One user who refused to settle faced a $ 22, 500 judgment. Bob Mehr, Gnat, Meet Cannon: Cecila Gonzalez Doesn't Want to Fight the Recording Industry. She Doesn't Have a Choice, Chi. Reader, Feb. 3, 2005, http://www.chicago reader.com/chicago/gnat-meet-cannon/Content?oid=917905. (accessed June 15, 2010).

239. Treacy, Bridget, Data Protection Law & Policy, 5 (March 2008).

240. Case C-275/06, Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU (Telefonica), 2008 E.C.R. 1-00271, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006J0275:EN:HTML. (accessed June 15, 2010).

241. Id.

242. Id.

243. Id.

244. Id.

245. Id.

246. Id. See also Treacy, Bridget, Data Protection Law & Policy, 5-6 (March 2008).

247. See infra. See also Eliot Van Buskirk, RIAA to Stop Suing Music Fans, Cut Them Off Instead, Wired, Dec. 19, 2008, http://blog.wired.com/business/2008/12/riaa-says-it-pl.html; Mathew Ingram, RIAA Drops Lawsuit Strategy for "Three Strikes" Plan, Gigaom, Dec. 19, 2008, http://gigaom.com/2008/12/19/riaa-drops-lawsuit-strategy-for-three-strikes-plan; Nate Anderson, RIAA Graduated Response Plan: Q&A with Cary Sherman, Ars Technica, Dec. 21, 2008, http://arstechnica.com/old/content/2008/12/riaa-graduated-response-plan-qa-with-cary-sherman.ars. (accessed June 15, 2010).

248. Mathew Ingram, RIAA Drops Lawsuit Strategy for "Three Strikes" Plan, Gigaom, Dec. 19, 2008, http://gigaom.com/2008/12/19/riaa-drops-lawsuit-strategy-for-three-strikes-plan (accessed June 15, 2010).

249. Nate Anderson, RIAA Graduated Response Plan: Q&A with Cary Sherman, Ars Technica, Dec. 21, 2008, http://arstechnica.com/old/content/2008/12/riaa-graduated-response-plan-qa-with-cary-sherman.ars. (accessed June 15, 2010).

250. Mathew Ingram, RIAA Drops Lawsuit Strategy for "Three Strikes" Plan, Gigaom, Dec. 19, 2008, http://gigaom.com/2008/12/19/riaa-drops-lawsuit-strategy-for-three-strikes-plan. (accessed June 15, 2010).

251. See id.

252. See id.

253. See Andrew Lyle, RIAA to Stop Suing Users, Cuts Them Off Instead, Neowin, Dec. 19, 2008, http://www.neowin.net/news/main/08/12/19/riaa-to-stop-suing-users-cuts-them-off-instead. See also Karl Bode, AT&T Wants Government Website Blacklists, Hadopi-Style Tribunal, May 3, 2010 at http://www.techdirt.com/articles/20100430/1423539264.shtml (accessed June 15, 2010).

254. 17 U.S.C. 512(j)(1)(A)(ii) (2006).

255. See id.

256. See id.

257. See id.

258. Jennifer M. Urban & Laura Quilter, 22 Santa Clara Computer & High Tech. L.J. 621, 639 (2006).

259. Sandrine Rambaud File-Sharing: Education and Punishment for Illegal File Downloads Under French HADOPI Law Electronic Commerce & Law Report: News Archive > 2010 > 05/19/2010 > BNA Insights at http://ezproxy.jmls.edu:2096/epln/EPLNWB/split_display.adp?fedfid=17191534&vname=eiplnotallissues&wsn=500636000&searchid=11625324&doctypeid=1&type=date&mode=doc&split=0&scm=EPLNWB&pg=0 (subscription required) (accessed June 15, 2010).

260. la Rédaction de Net-iris et publié le vendredi 15 mai 2009.Les missions de la Haute Autorité pour la diffusion des oeuvres et la protection des droits sur internet at: http://www.net-iris.fr/veille-juridique/actualite/22267/les-missions-de-la-haute-autorite-pour-la-diffusion-des-oeuvres-et-la-protection-des-droits-sur-internet.php(accessed June 15, 2010).

261. Sandrine Rambaud File-Sharing: Education and Punishment for Illegal File Downloads Under French HADOPI Law Electronic Commerce & Law Report: News Archive > 2010 > 05/19/2010 > BNA Insights at http://ezproxy.jmls.edu:2096/epln/EPLNWB/split_display.adp?fedfid=17191534&vname=eiplnotallissues&wsn=500636000&searchid=11625324&doctypeid=1&type=date&mode=doc&split=0&scm=EPLNWB&pg=0 (subscription required) (accessed June 15, 2010).

262. Id. see also "Hadopi: le Conseil constitutionnel censure la riposte graduée" (in French). *Le Monde*. 10 June 2009. http://www.lemonde.fr/technologies/article/2009/06/10/hadopi-le-conseil-constitutionnel-censure-la-riposte-graduee_1205290_651865.html. (accessed June 15, 2010).

263. Sandrine Rambaud File-Sharing: Education and Punishment for Illegal File Downloads Under French HADOPI Law Electronic Commerce & Law Report: News Archive > 2010 > 05/19/2010 > BNA Insights at http://ezproxy.jmls.edu:2096/epln/EPLNWB/split_display.adp?fedfid=17191534&vname=eiplnotallissues&wsn=500636000&searchid=11625324&doctypeid=1&type=date&mode=doc&split=0&scm=EPLNWB&pg=0 (subscription required) (accessed June 15, 2010). " [...] HADOPI 2 provides that a single judge may render a decision without informing the pirate and without any debate between the parties. However, as soon as the "pirate" receives the judge's decision, they may challenge this decision within 45 days, following which a traditional procedure shall be followed, in which the web user may defend their case."

264. Full text of the Act as amended and put into force available at "http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=3699621(accessed June 15, 2010).

265. "Controversial UK anti-piracy law finally passed". Telecoms Europe. http://www.telecomseurope.net/content/controversial-uk-anti-piracy-law-finally-passed?section=HEADLINE&utm_source=lyris&utm_medium=newsletter&utm_campaign=telecomseurope. Retrieved 9 April 2010.

266. Full text of the Act as amended and put into force available at "http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=3699621(accessed June 15, 2010), See Clause 18 on "Preventing access to specified online locations for the prevention of online copyright infringement".

267. Id. see also Charles Arthur Digital economy bill: what you need to know, Mach 22, 2010 at: http://www.guardian.co.uk/media/2010/mar/22/digital-economy-bill.

268. See By Ali Qassim april 2010. http://news.bna.com/pwdm/PWDMWB/split_display.adp?fedfid=16980236&vname=prabulallissues&wsn=499955500&searchid=11543456&doctypeid=1&type=date&mode=doc&split=0&scm=PWDMWB&pg=0 (accessed June 15, 2010).

269. See e.g open rights group Jim Killock, Digital Economy Bill: dangerous and draconian just got dictatorial 20 November 2009 http://www.openrightsgroup.org/blog/2009/digital-economy-bill; David Meyer, Open Wi-Fi 'outlawed' by Digital Economy Bill(accessed June 15, 2010). ZDNet UK, 26 February, 2010 at: http://www.zdnet.co.uk/news/networking/2010/02/26/open-wi-fi-outlawed-by-digital-economy-bill-40057470/ (accessed June 15, 2010).

270. UK Politicians Looking To Repeal Digital Economy Act from the *good-for-them* dept at Http://www.techdirt.com/articles/20100518/0900499464.shtml(accessed June 15, 2010).

271. Mike Mesnick New Zealand Copyright Minister Sneaks In 3 Strikes Law; Yells At Those Who Ask Why, Oct 10th 2008at http://www.techdirt.com/articles/20081009/2144022508.shtml(accessed June 15, 2010).

272. Mike Mesnick, New Zealand Moves Forward With Three Strikes; Big Questions Left Unanswered April 10, 2010 at: http://www.techdirt.com/articles/20100425/2121239163.shtml; see also NZPA Three strikes for online copyright abusers February 26, 2010 at: http://tvnz.co.nz/technology-news/three-strikes-online-copyright-abusers-3383024(accessed June 15, 2010).

273. Four strikes in the Belgium draft copy of the French Hadopi law, 24 March, 2010 at: http://www.edri.org/edrigram/number8.6/four-strikes-belgium(accessed June 15, 2010).

274. See generally Jeremy de Beer & Christopher D. Clemmer, Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?, 49 JURIMETRICS J. 375 (2009).

275. Genan Zilkha, Note: The RIAA's Troubling Solution to File-Sharing, 20 Fordham Intell. Prop. Media, &, Ent. L.J. 667, 701 (2010).

276. Greg Sandoval, AT&T First to Test RIAA Antipiracy Plan, CNET News, Mar. 24, 2009, http://news.cnet.com/8301-1023_3-10203799-93.html?tag=mncol;txt. (accessed June 15, 2010).

277. Verizon, Support, Announcements, https://www.verizon.net/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_announce ment&id=copyright (last visited Jan. 4, 2009) (accessed June 15, 2010).

278. Id. David Carnoy, Verizon Ends Service of Alleged Illegal Downloaders, CNET News, Jan. 20, 2010, http://news.cnet.com/8301-1023_3-10437176-93.html.

279. Id.

280. David Carnoy, Verizon Ends Service of Alleged Illegal Downloaders, CNET News, Jan. 20, 2010, http://news.cnet.com/8301-1023_3-10437176-93.html.

281. Amol Rajan, Virgin Warns Illegal Downloaders: Stop or Face Prosecution, THE INDEP., June 7, 2008, http://www.independent.co.uk/arts-entertainment/music/news/virgin-warns-illegal-downloaders-stop-or-face-prosecution-842086.html. (accessed June 15, 2010).

282. Lars Brandle, *ISPs On The Agenda At BPI AGM*, BILLBOARD.BIZ, July 9, 2008, http://www.billboard.biz/bbbiz/content_display/industry/e3i3a02b4b8960ca28a1cbaf4bafed07503. (accessed June 15, 2010).

283. Press Release, U.K., Dept. for Bus., Enter. & Reg. Reform, New Measures to Address Online File-Sharing (July 24, 2008), http://www.wired-gov.net/wg/wg-news-1-nsf/0/788A1-BAE10F752DB80257 490002B4756?OpenDocument (accessed June 15, 2010).

284. Net Firms in Music Pirates Deal, BBC NEWS, July 24, 2008, http://news.bbc.co.uk/2/hi/technology/7522334.stm.>ENDFN> (accessed June 15, 2010).

285. John Collins, Eircom to cut broadband over illegal downloads, , May 24, 2010, at http://www.irishtimes.com/newspaper/frontpage/2010/0524/1224271013389.html (accessed June 15, 2010).

286. Johnny Ryan, Three strikes, copyright and copytight? 24 April 2010 At http://johnnyryan.wordpress.com/2010/04/24/three-strikes-copyright-and-copytight/ (accessed June 15, 2010). "A case in the Irish High Court between Eircom and the Irish Recorded Music Association (IRMA) resulted in a settlement in January 2009. Under the agreement Eircom has committed to:

1. inform its broadband subscriber that the subscriber's IP address has been detected infringing copyright and

2. warn the subscriber that unless the infringement ceases the subscriber will be disconnected and

3. in default of compliance by the subscriber with the warning it will disconnect the subscriber."

287. John Collins, Eircom to cut broadband over illegal downloads, , May 24, 2010, at http://www.irishtimes.com/newspaper/frontpage/2010/0524/1224271013389.html(accessed June 15, 2010). see also Irish ISP Launches a Voluntary "Three-Strikes" Policy, May 26th, 2010 http://extratorrent.com/article/511/irish+isp+launches+a+voluntary+%E2%80%9Cthree+strikes%E2%80%9D+policy.html(accessed June 15, 2010).

288. For a detailed analysis of the benefits nad drawbacks of the graduated response scheme see Yu, Peter K., The Graduated Response (March 28, 2010). Florida Law Review, Vol. 62, 2010. Available at SSRN: http://ssrn.com/abstract=1579782; see also Genan Zilkha, The RIAA's Troubling Solution to File-Sharing, 20 Fordham Intell. Prop. Media & Ent. L.J. 667 (2010). "In a study by the University of Washington, three computer scientists found that the RIAA method of tracking illegal file-sharers and sending them takedown notices

was unreliable and "inconclusive." These scientists were able to convince the RIAA through manipulations that machines that were not sharing files actually were sharing files. The scientists also found that while some users were caught even though they were not doing anything illegal, other users could intentionally avoid being tracked. For example, the Pirate Bay, a widely used BitTorrent tracker, has offered a virtual private network ("VPN") subscription service, called IPREDator, that claims to mask IP addresses of subscribers so that they can escape RIAA detection. The University of Washington scientists further found that "it is possible for a malicious user (buggy software) to implicate (frame) seemingly any network endpoint in the sharing of copyrighted materials." A study by Google found that 57% of takedown notices it received under the DMCA were sent by business competitors who were trying to undercut each other, and that 37% of notices were "not valid copyright claims." The RIAA has even admitted that it has sent out mistaken takedown notices in the past. In a particularly embarrassing case, the RIAA sent a takedown notice to Penn State University, stating that someone in the "astronomy and astrophysics department had illegally uploaded songs by the artist [Usher] for free distribution" based on the existence of a file entitled "Usher." In reality, the file was an a cappella song uploaded by Professor Usher. After apologizing, the RIAA admitted that it had "sent out dozens of mistaken notices in the past, and at times, did not always fully confirm a suspected case of infringement." Faulty methodology thus undermines the strength of the RIAA's claims.

289. Peter K., Yu The Graduated Response (March 28, 2010). Florida Law Review, Vol. 62, 2010. Available at SSRN: http://ssrn.com/abstract=1579782, pp 15-17. (accessed June 15, 2010).

290. Sandrine Rambaud File-Sharing: Education and Punishment for Illegal File Downloads Under French HADOPI Law Electronic Commerce & Law Report: News Archive > 2010 > 05/19/2010 > BNA Insights at http://ezproxy.jmls.edu:2096/epln/EPLNWB/split_display.adp?fedfid=17191534&vname=eiplnotallissues&wsn=500636000&searchid=11625324&doctypeid=1&type=date&mode=doc&split=0&scm=EPLNWB&pg=0 (subscription required) (accessed June 15, 2010).

291. Swedish BitTorrent tracker the Pirate Bay available at: http://thepiratebay.org/(accessed June 15, 2010).

292. See IP Redator at: https://www.ipredator.se/?lang=en(accessed June 15, 2010).

293. Martyn Warwick TelecomTV: the Foolishness of Hadopi 2, the French Internet Law, March 16, 2010 at http://www.mediafuturist.com/2010/03/foolishness-of-hadopi-2.html (accessed June 15, 2010).

294. Id.

295. Peter K., Yu The Graduated Response (March 28, 2010). Florida Law Review, Vol. 62, 2010. Available at SSRN: http://ssrn.com/abstract=1579782, p 4 (accessed June 15, 2010).

296. Michael Geist, Australian Judge Explains Why Three Strikes Isn't Reasonable, February 03, 2010 at: http://www.michaelgeist.ca/content/view/4760/125/(accessed June 15, 2010).

297. Press Release, Agreement on EU Telecoms Reform paves way for stronger consumer rights, an open internet, a single European telecoms market and high-speed internet connections for all citizens, 5 November 2009 http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/491.

298. Id. see also A "FAQs on internet access safeguards and the telecoms package" document released Nov. 5 by negotiators is available at http://www.europarl.europa.eu/pdfs/news/expert/background/20091105BKG63887/20091105BKG63887_en.pdf. (accessed June 15, 2010).

    Further information on the new agreement, including the archived webcast of the press conference announcing the compromise package, is available at http://www.se2009.eu/en/meetings_news/2009/11/5/europe_united_on_telecoms_package?localLinksEnabled=false (accessed June 15, 2010).

299. Press Release, Anti-Counterfeiting Trade Agreement: European Commission welcomes release of negotiation documents 21 April 2010 http://trade.ec.europa.eu/doclib/press/index.cfm?id=552; see also David Meyer, Europe "Will Not Accept" Three Strikes in ACTA Treaty, ZDNET, Feb. 26, 2010, http://news.zdnet.co.uk/communications/0,1000000085,40057434,00.htm (accessed June 15, 2010).

300. Secretary Clinton: January 2010 Remarks on Internet Freedom at http://www.state.gov/secretary/rm/2010/01/135519.htm (accessed June 15, 2010).

301. Id.

302. Testimony of Rebecca MacKinnon Visiting Fellow, Center for Information Technology Policy, Princeton University Co-Founder, Global Voices Online (globalvoicesonline.org) http://www.internationalrelations.house.gov/111/mac031010.pdf (accessed June 15, 2010).

303. Id. see also part III.

304. See Ronald Deibert, China's Cyberspace Control Strategy, February 2010, discussing the case of "a recently leaked Cisco presentation from 2002 showing that company members viewed. China's then emerging censorship system (the so-called "Golden Shield") as a market opportunity, thus contradicting repeated claims made by the company that it is not morally responsible for sales of its equipment to regimes that censor and engage in surveillance" available at http://www.onlinecic.org/resourcece/archives/chinapapers (accessed June 5, 2010).

305. See Global Network Initiative at http://www.globalnetworkinitiative.org/corecommitments/index.php (accessed June 10, 2010).

306. Id. see also Testimony of Rebecca MacKinnon Visiting Fellow, Center for Information Technology Policy, Princeton University Co-Founder, Global Voices Online (globalvoicesonline.org) http://www.internationalrelations.house.gov/111/mac031010.pdf (accessed June 15, 2010).

307. H.R. 2271: Global Online Freedom Act of 2009, at http://www.govtrack.us/congress/bill.xpd?bill=h111-2271 (accessed June 5, 2010).

308. See also Bobbie Johnson Obama urged to punish US firms for aiding internet censorship 30 June 2009 at http://www.guardian.co.uk/world/2009/jun/30/us-firms-aiding-censorship (accessed June 15, 2010).

309. Roy Mark, Google China Dispute Revive Global Online Freedom Act, January, 17, 2010 at http://www.eweek.com/c/a/Government-IT/Google-China-Dispute-Revives-Global-Online-Freedom-Act-493296/(accessed June 15, 2010).

310. Civil liberties group The Electronic Frontier Foundation along with Google and numerous other public interest organizations and Internet industry associations have joined with

Yahoo in asking a federal court to block a government attempt to access a Yahoo! email account based on probable cause without a search warrant. Joins With Google and Others to Argue for Fourth Amendment Protection of Email at https://www.eff.org/press/archives/2010/04/13 (accessed June 15, 2010). See also EFF Joins With Internet Companies and Advocacy Groups to Reform Privacy Law Coalition Urges Updates to Electronic Privacy Statute to Reflect Web 2.0 World, March 3, 2010 at http://www.eff.org/press/archives/2010/03/30 (accessed June 15, 2010).

311. Id.
312. Brian Hindley and Hosuk Lee-Makiyama "Protectionism Online: Internet Censorship and International Trade Law, ECIPE Working Paper No. 12/2009, at: http://www.ecipe.org/protectionism-online-internet-censorship-and-international-trade-law/PDF (accessed June 15, 2010).
313. Annemarie Bridy, Why pirates (still) won't behave: regulating p2p in the decade after napster, 40 Rutgers L.J. 565, 570 (2009).
314. Id. at 600.
315. Id. at 601.
316. Id. at 603.
317. Id. at 609.
318. Id. at 605.
319. Id.
320. Id. at 606.

# The economic analysis of moral right

**Ioannis Kikkis**

Introducing a topic of the economic analysis of moral right is falling into a two-fold heresy. In most continental countries legal science is considered as an autonomous science and law professors are sceptical about the economics of legal rules[1]. Moreover moral right developed in Europe[2] as a legal device conceptually distinct from the economic right. It derives from natural law, safeguards the authors' and performers' non-economic interests that arise from the creative act and falls within the realm of personality right.

The economic analysis is a relatively new approach that applies methods of economics to laws. Economic concepts are used in order to explain the effects of laws, to assess the economic efficiency of legal rules and to predict which legal rules shall be promulgated. Law is a purpose-independent system designed to enable individuals to increase the predictability of each others' behavior and thus to better coordinate their affairs[3]. A basic assumption of the economic thinking is that firms and owners are acting with bounded rationality, in the sense that they want to maximize their profit and minimize any transaction cost. But the limited cognitive processing power of people, since it is impossible to assimilate all the information at our disposal and accurately work out the consequences of the available information, poses some limits on their ability to make a truly rational decision achieving such an end.

Copyright is a natural field of economic analysis, in the sense that copyright law is the most acceptable means for promoting efficient allocation of resources that result from the creative act. The "public good" character of intellectual works justifies the creation of intangible property rights for hindering the progress of "free riders"[4]. The cost of creating an intellectual work is often high while the cost of its reproduction and its distribution is rather low. Limiting the access to a work by providing a legal monopoly acts as an incentive for creating the work in the first place. Economic efficiency is achieved by striking a proper balance between providing the incentives for creators, on the one hand, and ensuring access to culture of the public as well as diminishing the administrative costs of copyright protection[5], on the other.

Moral right allows creators and performers to control the treatment and presentation of their work or performance by others. It is the master piece of a system that places the author at the center of the legal protection and offers some modi-

cum of power to performers. Many jurists are reluctant to an economic analysis that stresses the market in the focus of the legal rationale. It is not acceptable for them to reduce the author and the performer to a mere rational agent intending to maximize his profit, to interchange the nobility of a natural right with a legal protection of a professional and social status.

Nevertheless an economic analysis offers a more pragmatic approach of the legal concept, capable of revealing the hidden richness of the notion of moral right without understating its capacity to protect a wide range of different interests that matter to a variety of different stakeholders. Suffice it to mention the reinforcement of authors' and performers' bargaining power, the safeguard of a professional and social standing, the maintenance of the economic advantages of their reputation, the prevention of consumers' deception, the raising of a bulwark against dilution of natural culture[6].

For the purpose of this study aiming at the better systematic understanding of legal rules of moral right, I will focus at the situations of market failure that induced those rules (A) before assessing their economic efficiency (B) under a normative vision.

## Moral right and market failure

A perfectly efficient market requires full available information for all agents and free competition. Departures from this perfection, commonly known as market failures, would incur further costs for firms that want to trade intellectual goods and for users. Thus Copyright is justified by the presence of market barriers as high transaction costs, positive externalities, non-monetizable benefits or anti-dissemination motives[7].

Copyright is an answer to a form of market failure stemming from the presence of public goods, with two defining traits: the non-rivalrous use and the non-excludability[8]. An intellectual work is virtually inexhaustible, in the sense that anyone can simultaneously use a book without preventing others from using and without diminishing its value. Moreover, physical control of an intellectual work does not offer its usual potential as a mode of inexpensive enforcement for excluding free riders[9]. In a free market, there is no means to exclude those users that have not paid for access and use of the work. As a result of their "public good" character, intellectual works would have been under-produced if left to the free market.

Copyright legal system acts in diverse ways to restore the conditions of perfect competition and allow the market to function. Moral right becomes an instrument for promoting the efficient allocation of resources. In a market where information is incomplete or unreliable, moral right facilitates identification of the work`s owners, and thus makes easy to locate them and obtain further information on the validity

and duration of copyright claimed. Moral right influences the flow of information in a society in a different way than economic rights that affect the supply of available information. Its primordial role is to act on the information seeker's ability to judge the quality of the available information sources and to help him to choose between amongst competing sources[10]. Another economic function of moral right is to control reputational externalities to the potential benefit not just of the individual artists, but of other owners of the artist's works as well as of the public at large[11].

It is frequently argued that moral right embraces personal, non-pecuniary interests, totally distinct from the economic, commercial interests protected by Copyright. This is an affirmation partially true, because there is a strong imbrication[12] of pecuniary and non-pecuniary interests protected by moral right. From the point of view of acquisition, duration and international protection there is no difference between moral and economic right[13].

The long duration of moral right exceeding the artist's life is consistent with the view that moral right serve to support the value of the artist's work to society at large. The intellectual work after the death of the author acquires a collective dimension, in the sense that society has an interest that future generations could form an exact opinion of the work without being misled from the opportunistic actions of successive owners. Art collectors, museums and users are interested in the stability of meaning or value of cultural products. Damage to one of the author's work incur external costs for artist's other works and jeopardizes ideas socially valuable, such as persuasive statements of social critique or ideal contained in great works of art. This is the reason why after the artist's death some prerogatives of the moral right vest in a public authority[14].

The protection of author's and performer's pecuniary interests is also present while the artist exercises the moral right[15]. Forming a reputation as a capital of consecration implying the power to consecrate cultural products could be the only legitimate pretention of an artist but it is equally important that the artist profits from this operation. Therefore there is no paradox to claim that the exercise of moral right matters during negotiations for the exploitation of intellectual works and reinforces the bargaining power of the artist. There are several cases where pecuniary and non-pecuniary interests coincide. An unauthorized adaptation of the intellectual work could infringe both economic right and right of integrity. The right of disclosure could influence the exercise of economic rights and inversely the exploitation of the work could limit the moral prerogatives of the artist.

Moral right could be invoked by the artist to prevent an exploitation of a work in a way deemed to harm the reputation of the artist or without the appropriate attribution of the work to the creator. The name of the artist has acquired a market value[16] that is reflected in the market value of the work. It is in the artists' inter-

est to impede any depreciation of the reputation of their work by opportunistic adulteration of individual works[17].

Ultimately moral right could be defended as establishing legal assurances of the sources of works in order that the public may assess of those works and identify reliable and relevant information for their needs[18]. The right to integrity serves the interest of the society to maintain the meaning of intellectual works as construed by the author. The right to paternity or attribution is an exceptional symbolic means of appropriation of intellectual resources and functions in a similar way as a trademark. It is both a source of liability and an indicator of quality that operates in the public interest in so far as it increases the supply of information to consumers and thereby increases the efficiency of the market.

## Moral right and economic efficiency

Moral right provisions by striking a balance between the incentive to benefit from the commercial adaptation or exploitation of the work and the preservation of the social significance of the work foster the economic and social conditions necessary for efficient and effective information transfer flow. Moral right is also an instrument for promoting efficient allocation of resources. It is allocated to the persons that value more, authors and performers. From the point of view of productive efficiency, the results of the application of moral right could not be realized at a lower cost by application of another legal rule.

In the first place, free market and contractual mechanisms fail to produce an optimal amount of license agreements that preserve the integrity of an intellectual work. Creators fail to adequately account for the risks in their licensing decisions of the liberties that companies will take during the exploitation of their work and of the impact that these changes will have on the public. Since the interests in integrity are non-monetizable ones, creators have very little information regarding their fair value and they are reluctant to sacrifice a potentially lucrative market for the principle of moral right.

The existing remedies of a broad view of derivative works and unfair competition have not shown the same efficiency. It is true that taking a broad view of the derivative work may allow the author to protect many of the interests as the moral right. But this right could be transferred and cannot with the same force be opposed to the company-licensee of the author. Not to mention that in case of a work-made-for-hire copyright is vested in the producer. The protection provided by the legal rules of unfair competition could be of some help only in those cases that the degree of alteration is substantial and the altered version is so distorted that it makes no sense or results to the confusion of the public. Finally trademark law cannot adequately serve the interest of evaluating the authoritativeness of

information sources since the American Supreme Court held that trademark legal rules could not be used to enforce a claim which was essentially a moral rights claim for paternity *(Dastar Corp. v. Twentieth Century Fox Film Corp. et al.)*[19].

From the point of normative economic view rules of moral right seem to be efficient and improvement of existing law coincides with an expansive application of moral right to the common law system and the harmonization of moral right in the EU. Although in the 1995 Green Paper[20] the EC, considering the vital importance of moral right in a rapidly changing digital environment, had argued that the question of moral right was an urgent one, finally showed reluctance to any harmonization in this field. The reason advanced is that moral right has no incidence to the functioning of the internal market.

Questioning whether the differences of the legal rules of moral right in the EU MS could hamper the course of the functioning of the internal market, the Commission recognized that those rules have a significant economic impact[21]. Despite the EC's conclusion that there is no need for a priority action, I believe the differences are such significant that they will finish by disturbing the course of the internal market. The protection provided by moral right in the different EU states results to a significant imbalance, due to the inequality of the level of protection and the diametrical opposite solution of the issue whether and to what extent an author can waive his moral right[22]. The counter-productive and outdated absence of waivers in many EU MS could impose significant transaction costs for cultural industries arising from cumbersome negotiations or costly disputes. Isolation of markets and delocalization of cultural production with significant unjustified competitive advantages result from the fact that in the same market legal rules of moral right do not bind equally all entrepreneurs.

## Endnotes

1. G. De Geest, Law and economics in Belgium, http://encyclo.findlaw.com/0310book.pdf.
2. For the development from a legal concept of a natural and personal moral right until its effective protection, see I. Kikkis, Le droit moral de l'auteur dans la société de l'information, Thèse, Université de Nantes 2004, p. 11-16, E. Adeney, The moral rights of authors and performers, An International and Comparative Analysis, Oxford, 2006, p. 9-159.
3. T. Zywicki-A. Sanders, Posner, Hayek and the Economic Analysis of Law, http://www.law.gmu.edu/assets/files/publications/working_papers/07-05.pdf, p. 32.
4. R. Benko, Protecting Intellectual Property Rights: Issues and Controversies, Washington DC: American Entreprise Institute, p. 17. On moral rights see also Spinello R. & Bottis M., A defense of intellectual property rights, 2009.
5. W. Landes-R. Posner, An Economic Analysis of Copyright Law, http://cyber.law.harvard.edu/IPCoop/89land1.html, p. 1.
6. E. Adeney (n. 2 above), p. 3.

7. W. Gordon, Fair Use As Market Failure: A Structural and Economic Analysis of the Betamax Case and its Predecessors, Colum. L. Rev., 1982, vol. 82, p. 1627-1635.
8. R. Van den Bergh, The role and social justification of copyright: a law and economics approach, I.P.Q. 1998, p. 20.
9. W. Gordon (note 7 above), p. 1611.
10. M.A. Willkinson-N. Gerolami, The author as agent of information policy: The relationship between economic and moral rights in copyright, Government Information Quarterly 26 (2009) 321-332, p. 328.
11. H. Hansmann-M. Santilli, Authors' and Artists' Moral Rights: A Comparative Legal and Economic Analysis, Journal of Legal Studies January, 1997.
12. Imbrication between pecuniary and non-pecuniary interest means that moral right may serve to support the value of artist's work but it does not mean that it serves directly the pecuniary interests of the artist, in the sense that the artist can seek a double remuneration for both economic and moral right. We cannot adhere to the opinion of German specialists that moral rights might serve eventually even mainly pecuniary interests (A. Dietz, in Schricker Kommentar, Vor §§ 12 ff, n. 12). See also A. Bertrand, Le droit d'auteur et les droits voisins, 2nd edition DALLOZ, 1999, n.1.532.
13. G. Koumantos, Copyright, 7th edition, Sakkoulas, Athens, 2000, p. 34: Copyright is unitary from the point of view of acquisition, duration, international protection and the sum of two distinct rights from the point of view of transmission and limitations.
14. It is the case in Denmark and Sweden for the right of integrity if cultural interests are involved (art. 53 of Danish law, art. 51 of Swedish law), in Spain Italy, Portugal and Greece for the right of paternity and the right of integrity (art. 25 of Spanish law, art. 23 of Italian law, 56 par. 2 and 57 of Portuguese law and art. 29 par. 2 of Hellenic law).
15. It is worth noting that pecuniary interest is considered for the evaluation of the damage caused by the infringement of moral right, i.e. the omission of the name of the architects CA Paris, 20 oct. 1995, JurisData n.023723. If it is true that the exercise of the right of integrity could serve a pecuniary interest, the reasoning shall not be pushed too far by admitting that pecuniary motivation could justify the exercise of the moral right.
16. A. Berenboom, Le Nouveau Droit d'Auteur, LARCIER, 2nd edition, 1997, n. 99.
17. R. Van den Bergh (note 8 above), p. 30.
18. M.A. Willkinson-N. Gerolami (note 10 above), p. 329.
19. M.A. Willkinson-N. Gerolami (note 10 above), p. 330.
20. Green Paper 19 July 1995, COM (95) 382 final.
21. EC Communication of 20/11/1996, COM (96) 568 final, p. 27.
22. W. Grosheide, Moral rights, in E. Derclaye, Research Handbook on the future of EU Copyright, Cheltenham 2009, p. 265, J. de Werra, The moral right of integrity, in E. Derclaye, Research Handbook on the future of EU Copyright, Cheltenham 2009, p. 274, I. Kikkis, (note 2 above), p. 256-258. See also Spinello & Bottis, A defense of intellectual property rights, Edward Elgar Publishing, 2009.

# The Information Society law in Japan

**Munenori Kitahara**

## Introduction

About 50 years have passed since the information society was born in Japan. At the first term, the society was called a computerized society, or a computer society. It was called an information-oriented society, or an information society and an advanced information society. People might read a cultural fragrance in information rather than in computers as machinery. With telecommunication devices of networks, the information society was changed into an advanced information society and an advanced information network society. Today we live our lives in ubiquitous society, or smart ubiquitous society. Anyone who has an information terminal, can access the Internet at any time and anywhere.

Since 1990s, a new computing concept has been spread in all over the country and the Internet has been popularized in the people. Information accidents have rapidly increased in number on the information superhighway since then.

In Japan in 2000-01, the information and communications technology revolution has generated particularly strong interest. Clearly positioning IT as an important strategic issue, the Japanese government is undertaking various programs to ensure its advance. Japanese society as a whole has strong expectations that IT, as the basis of development in the new century, will spur reform of the nation's economic framework and bring greater efficiency to industry and allow for diversification of people's lifestyles and enhance the convenience of their daily activities.

In cooperation with the IT revolution, information society laws were established: unauthorized computer access act (1999); the information society formation act (2000); the combined communications and broadcasting act (2001); revised communications business act (2001); the electronic signatures and certification business act (2000); The electronic consumer contracts act (2001); the revised criminal act (2001).

Fortunately we Japanese could have the Basic Act on the Formation of an Advanced Information and Communications Network Society in 2000. In this Act, advanced information and communications network society means a society in which creative and vigorous development can be achieved in all fields by obtaining, sharing or transmitting globally a wide variety of information or knowledge

in a free and safe manner via the Internet and other advanced information and telecommunications network. The Basic Act provides for basic principles and a basic policy on the development of strategies with respect to the formation of the society, and determines the responsibilities of the Government and local public entities, and provides for the development of a Priority Policy Program on the formation.

This Basic Act shall describe a grand design of information society, and the other information society laws shall contribute a secure running of the society from every respect. In a word, the information society law shall prevent information accidents, and protect the rights and profits of peoples' of the 21st century.

## The Information Society of Japan

The information society of Japan can be divided into five terms. The first formation term(1965-1984) is chronologically composed of a computer society, a main computer society, a code number society, a card society and a databank society. The second growing term (1985-1990) is chronologically composed of a new media society, a network society, a multi-media society, an IC-card society, and a personal computer society. The third progressing term (1991-2002) is chronologically composed of the Internet society, an IPv.4 society, a grid computing society, e-Japan society and a handy phone society. The fourth developing term (2003-2007) is also chronologically of a P2P society, a cyberspace society, a wireless society, a Web2.0 society and u-Japan society. The fifth matured term (2008-2010) is chronologically composed of a ubiquitous society, an IPv.6 society, a twitter society, a virtualization society, and a cloud computing society.

Each term and sub societies are characterized by the information technologies of the ages. Politics and political economy could select the technologies. But all the information technologies have continued to be used until today as having been changed in the shape. No technologies have been dead.

Information society is a multi-faced society. The information society has many sub societies, from a computer society, a card society, a databank society, a personal computer society, a cyberspace society to a ubiquitous society, an IPv.6 society, and a cloud computing society. People can move, live, play and work in the sub societies.

Present society is also a multi-faced society. There are many societies in the present society, too. An agricultural society, an industrial society, a fishing society, an automobile society, a convenience stores society and an information society. Information society is only one of sub societies in the present society. Most people think that the present society is wholly an information society, because

computers and networks are used in all the sub societies. While people are making cars, they work in the industrial society. While people play and work with computers and networks, they live in the information society. People won't be able to call information society a society where there are neither computers nor networks. People can move various societies according to their roles.

## Information Society and Law

### *Technology and Law*

Information society a technological society which is an infrastructure of computer, communication, software and networking technologies. Generally speaking, an information technology should make more seven times rapid than a legislation technology. Because ICT has an electronic rapid and law has a paper rapid. Laws would walk after technologies. It is always law's fate to be left behind by technologies. It is particularly serious for laws not to control a security standard of using technologies.

### *Technology, Security and Law*

In many cases a law has anything to do with a technology, the law would provide the security standard of technologies. At the same time, the law also would provide the structure standard of technologies. In most technologies, a security standard would be reflected in the security standard.

### *Absolute Security and Relative Security*

In using a technology, when there should not happened an accident even if anyone at anytime and anywhere, it may be said that the technology has the absolute security. The technology is perfect from a viewpoint of security. But such a technology cannot be imagined. Technologies would have some defect from a standpoint of the users. Users are using technologies considering the defects lest they should come across accidents. They might be in accidents if they use wrongly the technologies. But, there should not occur any accidents by the ordinary using. This is relative security. So, laws would require technologies of the relative security.

## Information Technology and Information Accidents

### *Information Technology and the Defects*

All the technologies that we would use today have a kind of defects. But the technical experts willingly would never accept the words. I don't believe in the existence of a perfect technology with no defects. The technological progress means the efforts to reduce the effects as far as possible.

Computer, information, communications, and networking technologies, these technologies are being utilized in most wide-ranging. Even if these ICT's are utilized in laboratories, they would not cause problems. However, various problems have realized, as soon as those technologies appeared in our society. The defects of information technologies have seized the users with its fangs. The end-users have little knowledge of ICT. And they have no idea of ICT defects.

## *Defective Technologies and Information Accidents*

There can be found defects even in computer systems and networks. Those defects might be so-called security holes, which can be called the vulnerability and the weak points. Depending upon the defects, not only do the users receive damage, but also there is a possibility of causing damage to the other users. These are the information accidents.

## *Information Accidents*

Acceptable Use Policy existed in the Internet before. Then the use was limited to research and educational purposes. In a word, business was not able to be performed in the Internet. At that time there were few information accidents. In 1990's, the Internet was opened to business purposes and the user's limitation was removed in fact. The policy was abolished. Then the situation changed suddenly. The information accidents increased rapidly. It is because the user who doesn't know the Internet technology has participated in the Internet all at once.

The information accident is the incident on the Web, where the Internet users' rights and profits are violated. The information accidents occurs on the information superhighway same as the traffic accident does on the highway. The information accidents are collisions. Most of the information accidents are in collision with the principles of the constitution and the important principles of the social life.

a. Collision with freedom of expression

b. Collision with free speech

c. Collision with right of privacy

d. Collision with copyright law

e. Collision with right to data protection

f. Collision with contract law

g. Collision with criminal law

h. Collision with unauthorized computer access law

i. Collision with minor protection law

j. Collision with information security

k. Collision with business ethics

l. Collision with network etiquette

m. Collision with computer systems

## Information Society Law

### *The Meaning of Information Society Law*

The place where people use computers and networks is in the information society. People live their information lives in the society. In the present age, an information society is also a part of the modern society, as well as an industrial society, an agricultural society, a fishing society, and a convenience stores society. And people often should move to these societies through their long lives. Even in an information society, people move to the Internet society at some time, a blog and twitter society, a cloud society at another time. They should return to their home in the information society if the work or the recreation ending.

There are, in fact, formed an internet society, a cyberspace and a cloud society in computers, blade servers. The apparatus are installed in information society. The societies are so-called logical world which are virtualized in the server computers. The internet business is regulated by Telecommunications Business Law, which also controls a normal telephone business. Because the Internet uses a part of a telephone circuit. In that sense, the Internet is only a way of telecommunications between the Internet users. The contents in the Internet are regulated by Copyright Act. An unauthorized computer access is prohibited by Act on the Prohibit on an Unauthorized Computer Access. These acts have already been in force in the information society.

Today we may see various names of the legal system which relates to the Internet, networks, and computer systems. For example, "Multimedia Law," "Information Law," "The Internet Law," "Cyber Law," "Cyberspace Law," "Information Security Law," or "Cloud Law," "Cloud Computing Law." But all these laws regulate and control the information life. Therefore, all the laws could be introduced into the system of information society law.

### *The Characteristics of the Information Society Law*

#### Reflection of Computer System in Social System

The concept of computer system is composed from three main ideas: downsizing; open system; distributed processing; networking; end-user computing.

The downsizing in social systems reflects in a small government which reduces administrative cost by shaving many auxiliary organizations and refraining from the employment of the government employee. The distributed processing and end-user computing will try to change centralized politics to decentralization of power. Then local governments will have an authority of self-determination excluding military and international affairs. The open system and networking will contribute the standardization of local areas by exchanging information through networks.

## Information Technology Controlled with the Information Technology

The infrastructures of information society are "information," "information processing devices," and "information circulation routes." Software and contents technologies will relate to the information. Computer and machine technologies will relates to the devices. Networking and internet technologies will relate to the routes.

The information society law should introduce the information technologies in order to raise the effectiveness of the law itself. This introduction might be permitted only to the information society law. This means that information technologies should control themselves in the law. It is really the fusion of technology and law.

## The Fusion of Technology and Law

The Electronic Signatures and Certification Business Act has introduced encryption technologies. The purpose of this Act is to provide the presumption of authentic establishment of electromagnetic records by electronic signatures. In the Act, any electromagnetic record that is made in order to express information shall be presumed to be established authentically if the electronic signature is performed by the principal with respect to information recorded in such electromagnetic record. The authenticity and electronic signature of the electromagnetic record can be verified by the public key criptosystem.

In the Act Concerning Environment for Children to Safely Use the Internet, information providers shall be obliged to provide filtering technologies. This Act focuses on measures to protect minors from harmful information and explicitly provides for the direction of future efforts with respect to a vision of the environment for Internet utilization.

## *The System of Information Society Law*

The system of information society law should be the driving force to build and develop the information society of the 21st century. In 2001, we, Japanese could have Basic Law on the Formation of an Advanced Information and Telecommuni-

cations Network Society. In the legal system, the other information laws will be arranged under this Basic Law.

## Information Society formation Law

The purpose of this law is to provide for basic principles and a basic policy on the development of strategies with respect to the formation of an advanced information telecommunications network society, to determine the responsibilities of the Government of Japan and local public entities, to establish the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society and to provide for the development of a Priority Policy Program on the formation of an advanced information and telecommunications network society in consideration of the urgent need to appropriately keep pace with the rapid and drastic changes on a global scale in the socio-economic structures arising from the use of information and telecommunications technologies, to swiftly and throughly introduce the measures for the formation of an advanced information and telecommunication network society.

* Basic Act on the Formation of an Advanced Information and Telecommunications Network Society
* Basic Act on Intellectual Property
* Act on the Promotion of Information Processing
* Basic Act on the Protection of Consumers

## e-Government and e-Local Governments Law

This Law shall decide on the e-Government and e-Local Government that stipulates concrete efforts by the governments relating to the building of e-government. On the basis of this program, the governments are tackling business reform to improve the convenience of the public and services and respond to the spread of IT. The purposes of the e-governments are to put almost all the procedures relating to application, notification handled by administrative organizations of the state online, and to make efforts in a strategic and cross-sectional manner toward the simplification, greater efficiency, and rationalization of administrative operation through the optimization of business and systems, the government conducted a systematic rearrangement of the business and systems of the government as a whole.

With regard to performing administrative procedures online, the Act Concerning the Use of Information and Telecommunications Technology on Administrative Procedures came into force in 2003, and the development of systems including a government public key infrastructure (GPKI) and a general-purpose reception system was completed by the end of fiscal 2003. The development of an environ-

ment for performing administrative functions online is basically complete including the Basic Resident Registers Network System becoming fully operational in 2003 and the start of a public personal certification system that operates online, as well as electronic payment services for payment of taxes and various administrative fees in 2004.

The Local Government Wide Area Network(LGWAN), which is an administration-dedicated network connecting local governments, was connected with the intranets of prefectures and ordinance-designated cities and with e-Government Kasumigaseki WAN Network. The Basic Resident Register Network System went into full-scale operation. The Basic Resident Register IC card as serving as a public identification certificate is playing an important role as the basis of e-government and e-local government as well as the system.

In addition, during 2003, all local overnments bodies began participating in the Local Government Wide Area Netwrk (LGWAN). Using this environment, the online filing of most applications and notifications handed by central government agencies became possible by the end of fiscal 2003.

## Online Administrative Procedures Law

This law has made possible sending by e-mail, for applications, submissions, and notifications where administrative organizations are the main entity or addressee.

With regard to acceptance of online administrative procedures all administrative procedures including applications and notifications by individuals and companies will be made accessible around the clock from home and office computers via the Internet. In the area of legal systems, the three acts for providing online administrative procedures, namely, the Act Concerning the Use of Information and Telecommunications Technology on administrative Procedures, the Act Concerning Preparation of Related Acts for Enforcing Online Administrative Procedures Act, and the Act Concerning Digital Signature Certification of Local Public Entity (Public Individual Cerfication Act) for further comuterizing the central and local governments passed the Diet in 2002.

Furthermore, in order to enable application, report and other procedures to local governments available on the Internet, Government developed a certification infrastructure for organizations that was compatible with the Government Public Key Infrastructure (GPKI).

An electronic certificate from the Public Certification Service for Individuals (JPKI) service is valid for five years. It is issued by being sotored in a smart card such as the Basic resident Register card after strict personal identification process.

## E-Document Law

Of finance and tax related documents and ledgers required by law to be stored by private businesses, for those for which electronic storage is not approved, this law shall enable electronic storage of these documents and ledgers while ensuring credibility and visibility according to the contents and nature of the documents and ledgers based on the advance of information technologies. And this law shall approve the electronic storage of ledgers input on the computer without printing on paper.

* Electronic Ledger Act
* Act on Use of Information Communication Technology in the Storage of Writing by Private Businesses

## Information Circulation Law

This is a law which relates to the circulation of information in the information society. The law regulates a type (telecommunications or broadcast) of circulation, a way of circulation, a circulation technology, circulation apparatus.

The term "convergence of telecommunications and broadcasting" refers to a variety of phenomena accompanying digitization and broadband. These phenomena include progress in the online distribution of image and sound contents, sharing of terminals, and networkss, and cross entry between telecommunications and broadcasting. In the future, it is expected that the convergence will accelerate, and will new entry and the development of new competition are expected to make this convergence a new, leading industey which will contibute to economic growth.

Digital technology has seen siginificant progress, and the communication capabilities of networks have drastically risen through the use of broadband; the communications are now available both to telecommunication service and to broadcasting service.

In 2002, the Law Concerning Broadcast on Telecommunications Service was enacted, setting legal stipulations for broadcasting using telecommunications services.

In 2009, comprehensive proposals were made concerning the establishment of the new act on convergence, the review of regulations related to telecommunications, the deregulation of broadcasting, and other topics, which targeted the year 2011 when the world's most advanced infrastructure of telecommunications and broadcasting will be completed,toward achieving the goal of becoming a "broadband, mobile, and television superpower" in which Japan can exercise its strength.

## Information Property Law

The purpose of this law is to promote measures for the creation, protection and exploitation of information property in a focused and systematic manner by stipulating the basic principles on the creation, protection and exploitation of information property and the basic matters to achieve the principle, clarifying the responsibilities of national government, local governments universities and business operators, providing stipulations on the development of a strategic program on the creation, protection and exploitation of information property.

* Intellectual Property Act
* Copyright Act
* Act on the Creation, Protection and Exploitation of Information Contents

## Electronic Contracts Law

In the efforts to remove impediments to the IT revolution, the Japanese government has revised components or the regulatory system to allow private-sector transactions to take place via e-mail as well as by the traditional exchange of paper documents.

The Electronic Signature and Authentication, which came into force in 2001, was enacted to give legal status to electronic signatures as a means of verifying that the other party in an e-commerce transaction is really who he or she says he is and to create a national approval system for electric certification operation.

## Information Freedom Law

The purpose of this law is to endeavor towards greater disclosure of information held by administrative organs thereby ensuring to achieve accountability of the Government to the citizens for its various activities, and to contribute to the promotion of a fair and democratic administration that is subject to the citizens' appropriate understanding and criticism.

* Act on Access to Information Held by Administrative Organs
* Act on Access to Information Held by Incorporated Administrative Agencies
* Act Concerning the Promotion of Business Activities with Environmental Consideration by Specified Corporations etc., by Facilitating Access to Environmental Information, and Other Measures
* Pollutant Release and Transfer Register Act

## Personal Information Protection Law

The purpose of this law is to stipulate the basic concepts and the basic policies of the Government regarding the proper handling of personal information and other basic matters in connection with the protection of personal information, to clarify the duties of the State and the local governments in relation therewith, and to protect the rights and interests of individuals by stipulating the obligations to be complied with by the businesses handling personal information while taking the usefulness of personal information into consideration.

* Personal Information Protection Basic Act
* Act on the Protection of Personal Information Held by Administrative Organs
* Act on the Protection of Personal Information Held by Independent Administrative Agencies

## Information Protection and Preservation Law

The purpose of this law is to secure the key concepts of information security. Confidentiality of information ensures that only those with sufficient privileges and a demonstrated need may access certain information. Integrity is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or their disruption of its authentic state. Availability is the characteristic of information that enables user access to information without interference or obstruction and in a useable format.

The Provider Liability Limitation Act was enforced in 2002 as a measure against increasing cases of information violation of the rights of others on a website or BBS. This Act provides limitation and clarification of damage liability of providers in cases where the rights of others are violated and the rights of a person whose rights have been violated to demand the provider to disclose the information source.

The Law on Identification of Cellular Phone Users by Mobile Operators and Prevention of Abusive Use of Cellular Phones obliges mobile phone operators to conduct identity verification when concluding contracts or transfer to prevent the abuse of mobile phones.

Since the Act on Regulation of Transmission of Specified Electronic Mail includes a provision whereby telecommunication operators can refuse the false e-mail address, it can also be effective as a countermeasure against phising.

### Internet Young User Protection Act

The formal name of the Act is " Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People." The purpose of this Act, in light of the situation where content harmful to young people is distributed extensively on the Internet, is to contribute to the protection of the rights of young people by providing them with safe and secure Internet use through taking measures necessary for young people to acquire skills for the appropriate utilization of the Internet as well as improving the performance and disseminating the use of software for filtering content harmful to young people and any other measures, etc. for reducing the chance of young people viewing content harmful to young via the Internet as much as possible.

### Information Criminal Law

The law prohibits information crimes, that is, cybercrime, computer crime, network crime and card crime. Cybercrime is offenses against the confidentiality, integrity and availability of computer systems networks and computer data as well as the misuse of such systems, networks and data according to Convention on Cybercrime (Council of Europe). The types of the crime are illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, content-related offenses, and offenses related to infringements of copyright.

The types of computer and network crimes are unauthorized creation and use of electromagnetic records, computer fraud, damaging of documents for government use. The types of cards crimes are unauthorized creation of electromagnetic records of payment cards, possession of payment cards with unauthorized electromagnetic records, and preparation for unauthorized creation of electromagnetic records of payment cards.

## Conclusion

I would not intend to rearrange information laws with the title "the information society law," unless we, Japanese, had the information society formation basic act. In the system of information society law, the basic act occupies a central position. Because the act describes a grand design of an advanced information and communications society, a ubiquitous network society of the 21st century.

So far, laws would chase after technologies. Some time lag always would exist between law and technology. But there may be a possibility to recover the time lag in the information society law. The law can have a technology control the

technology itself. This is just a fusion of law and technology. The very fusion would appear in the information society law of the 21st century.

## References

M.E. Whitman&H.J. Mattord (2008), Management of Information Security (2nd ed.), Thomson.

Éditions UNESCO/ECOMICA (2005), Les Droits de l'homme dans le cyberspace, Paris.

J. Armitage & J. Roberts (2002), Living with Cyberspace: Technology & Society in the 21st Century, continuum.

D. Baumer & J.C. Poindexter (2002), Cyberlaw and e-commerce, McGraw-Hill.

J.E.J. Prins (ed.) (2001), Designing E-Goverment, Kluwer Law International.

Y. Akdeniz, C. Walker & D. Wall (eds.) (2000), The Internet, Law and Society, Longman.

C. Féral-Schuhl (2000), Cyberdroit, Dunod.

S. Engel-Flechsig & A. Roßnagel (hrsg.) (1998), Multimedia-Recht, Beck Texte.

T. H. Strömer (1997), Online-Recht: Rechtsfragen im Internet, 2., aktualisierte u. erweiterte Auflge, dpunkt.verlag.

C. Gringras (1997), The Laws of the Internet, Butterworths.

G. JH Smith (1996), Internet Law and Regulation, Bird & Bird.

M. Kitahara (2010), The Concept of Personal Data Protection in Information Society, Social Systems Solutions by Legal Informatics, Economic Sciences and Computer Sciences, Kyushu University Press.

M. Kitahara (2008), The Information Technology and Ethical Use, Kyushu University Press.

# New rules on consumer protection against personal data breaches and spam

**Panayiots Kitsos**

## Introduction

The rapid evolution of Information and Communication Technologies has significantly altered the way information is being stored and used. In particular, as noted by Yves Poullet, the development of information technology is characterized by three elements: firstly, the constant growth of the capacity of computers, user terminals and the communication infrastructure (the so-called Moore's Law), secondly, the Internet revolution, and the subsequent convergence of the network around a single interoperable platform, the appearance of the 'Semantic Web' and Web 2.0 and the changes in identification and authentication techniques and thirdly, the emergence of ambient intelligence that merges technology and the network and puts that technology into our everyday life, [Yves Poullet 2009].

Especially the use of the Internet and electronic filing systems have changed dramatically the way personal information is being viewed, by all sorts of entities such as universities, schools, hospitals, government agencies, corporate entities, and individuals, allowing virtually anyone to access vast amounts of information regarding personal data [Clifton 2009]. As noted "information....has passed from being an instrument through which acquire and manage other assets to being a primary asset it self" [Gindin 1997]. Corporations and marketers are collecting data which "extend beyond information about consumer's views of the product to information about consumers themselves, often including lifestyle details and even a full-scale psychological profile" [Solove 2004]. Social security numbers, credit-card numbers, medical records, e-mails and every information that can be defined as personal data can now easily be stored, processed, for illegal purposes or from unauthorized third parties. As a result data breaches and identity theft threaten privacy of citizens and often result in considerable costs for business and other organizations.

The collection of these types of data is made possible with the help of the so-called "cookies", which "have often been associated with potential security breaches, unauthorised transaction monitoring and privacy breaches" [Mitrakas 2006].

"Cookies" are small pieces of text files that are sent and placed by web servers to a user's computer, so that the users may be identified every time they log on to that web server enabling web sites to be personalised by remembering the users preferences [King 2003] . The information that is collected does not necessarily identify a specific individual. "However, when combined with on-site registration data, which the Internet user provides when visiting some sites, cookie data may be used to build a profile of the specific Internet user" [Gindin 1997]. The main arguments against cookies is that internet users are unaware of cookies and that their personal data is being collected, without their prior knowledge or consent usually for direct marketing purposes [Munir 2005].

In addition to these internet technologies posing a threat to privacy, the unwanted e-mail marketing (the so-called "spam") which has been defined as "(...) the bulk-mailing, sometimes repeatedly, of unsolicited e-mail messages, usually of a commercial nature, to individuals with whom the mailer has had no previous contact and whose email addresses the mailer collected from the public spaces of the Internet: newsgroups, mailing lists, directories, web sites etc" [CNIL 1999, Gauthronet, Drouard 2001], is a constant cause of unease for regulators and consumers.

Still, data security breach and identity theft are regarded as one of the most important threats to privacy, which has a severe effect on the evolution of Information Society.

On May 28, 2010, the UK Information Commissioner's Office issued a press release stating that it has been notified of more than 1,000 data security breaches since it began keeping records in late 2007(U.K's Information Commissioner Officer). This incident which was just one in a series of data breaches in UK raised the question first, of the need to view and manage data security at an organization wide level, and treat the problem as a priority by senior management. Secondly, that "while organizations generally understand that technology is a business enabler, they are still failing to recognize that it is also a risk" [Turle 2009].

Another recent data security breach event took place in Finland where data that were stolen from an Helsinki business in January 2010 exposed more than 100,000 payment cards. A small number of the compromised cards have been used to conduct fraudulent transactions.

These cases are just an example of the immensely growing problem of data security breach and identity theft. Indentity theft is the fastest growing type of fraud in the United States. In 2008, about 9.9 million Americans were reportedly victims of identity theft, an increase of 22% from the number of cases in 2007 [Bottis, 2010]. These incidents raise consumers concerns over the possibility of misuse of their per-

sonal data resulting thus to lower confidence in internet transactions. Consumer confidence can then be gained only when electronic communication and internet service providers enhance security features of their services [Finklea 2010].

The problem is attempted to be addressed through a system of notification of those breaches. Notification has been seen as an important way towards the development of data security since it has been driving investment in data security within provider entities and allowing affected individuals to mitigate their damages [Dhont Woodcock 2010]. Nitigation is possible by alerting their bank, their credit card merchant, the National Regulatory Authority and law enforcement agencies; 'they can close unused financial accounts; they can place a credit freeze or fraud alert on their credit report", not to mention that these notifications "can also enable law enforcement, researchers, and policy makers to better understand which firms and sectors are best (worst) at protecting consumer and employee data" [Romanosky, Telang, Acquisti 2008].

Moreover the right to be notified, as the right of the consumer to know when their personal information has been stolen or compromised [Maurushat 2009], is enabling individuals to take steps to protect themselves from any harmful effects of the breach. Other justifications include the increase of "accountability" of organizations that suffer breaches, rising "awareness among the public" and "allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints" [Cate 2008].

In U.S.A various Data Breach Notification laws exist. The first State to have enacted data breach notification laws was California with the California Computer Security Breach Notification Act (S. B 1386), which came into effect on 2003. Since then, most of the States have introduced similar laws . As a result, U.S and international companies started to be more careful when using personal data, realizing that lack of security measures could seriously jeopardize their reputation and business.

In Europe, even though data privacy has been heavily regulated offering European citizens an adequate legal framework to protect their personal data, still, prior to the new amended e-privacy directive, European consumers had no right to know "when their information has been tampered with or leaked illegitimately to a third party as the result of a security breach" [Cooper, Fink, Jones, Van Quathem 2006].

The growing numbers of data breaches led European Union to recogne the importance of identifying and managing data breaches via the existing legal framework.

On 25 November 2009, the European Parliament and the European Council adopted a new legislation to revise the regulatory framework for the electronic

communications sector. This legislation includes Directive 2009/136/EC, which amends earlier Directive 2002/58/EC in the fields of 1. mandatory notification of personal data security breaches, 2. consent requirements for cookies and 3. anti-spamming measures by ISPs.

The scope of the Directive is to enhance the protection of consumers privacy and personal data in the electronic communications sector, through strengthened security-related provisions and improved enforcement mechanisms by the NRAs .

## Data security law in the European Union

Data Security in the European Union has been regulated by two Directives: Directive 95/46/EC,("Data Protection Directive"), and the newly amended Directive 2002/58/EC,4 on ("Privacy and Electronic Communications Directive").

### *Directive 95/46/EC*

In the Data Protection Directive, article 17(1) of the Data Protection Directive requires the "controller" processing personal data in the European Union to implement "appropriate technical and organizational measures" to protect any personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

In particular, the Directive states that "having regard to the state of art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected".

According to Cooper, Fink, Jones and Van Quathem, the use of the word "appropriate" is in line with the scope of the Directive. "This was, however, intentional, since otherwise any specific security provisions rapidly would have become outdated. Instead, the Directive merely requires organizations to consider available technologies, their associated costs and the harm that would arise from unauthorized disclosure of or damage to personal data. In other words, organizations processing sensitive personal data will be expected to put in place more robust security measures" [Cooper, Fink, Jones, Van Quathem 2006].

Article 17(2) sets out additional conditions requiring the data controller "where processing is carried out on his behalf" to choose "a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures"

Article 17 (3) stipulates that the carrying of the processing has to be done by a written contract or other binding legal act in place between the data processor and any third party that processes personal data on its behalf.

### *Directive 2002/58/EC*

Directive 2002/58/EC supplements the Directive 95/46EC aiming at protecting the fundamental right of privacy of natural persons in the field of electronic communication services also ensuring the free movement of such data in the Community.

Article 4 of the Directive restates the provisions of Directive 95/46/EC requiring providers of a publicly available electronic communications service to take appropriate technical and organizational measures to safeguard security of their services. In paragraph 2 we provides for the mandatory alert of observe that Directive the subscribers by the providers of a publicly available electronic communications service in case of a particular risk of a breach of the security of the network.

However, the Directive does not impose any "obligation to inform or notify the consumers of an actual breach, such as, for example, theft of credit card information"[Cooper, Fink, Jones, Van Quathem 2006].

The need for Europe to enhance internet security and tackle data breaches through security breach notification systems that had already been introduced in U.S.A started to be more than urgent and led to an intense debate that resulted to the new e-privacy directive provisions.

## The new E-privacy Directive

As amended by Directive 2009/136/EC the new E-privacy Directive introduces an obligation to notify individuals and authorities in instances of information security breaches.

### *Personal data breach*

The Directive 2009/136/EC adopts the concept of "personal data breach" which according to the Directive is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community" [Directive 2009/136/EC].

"Personal data" is defined as any data relating to an identified or identifiable individual, which is any data that may be linked to individuals through other information even where that information is held by another person [Directive 95/46/EC].

Under the second opinion of the European Data Protection Supervisor this definition is welcome "insofar as it is broad enough to encompass most of the relevant situations in which notification of security breaches might be warranted". [EDPS 2009]. In addition, the EDPS stresses that this definition could "also include situations where there has been a loss or disclosure of personal data, while unauthorized access has yet to be demonstrated". As an example of possible personal data losses, according to the EDPS are CD-ROMs, USB drives, other portable devices or other situations where personal data have been made publicly available by regular users such as employee data file made inadvertently and temporarily available to a publicly accessible area through the Internet.

It is important though to make a reference to the definition of personal data according to the above mentioned "California Computer Security Breach Notification Act". The Act defines "personal information" as an individual's first name or initial and last name in combination with one or more "data elements," if either the name or the data elements are not encrypted. These data elements are: social security number (SSN); driver's license or state identification card number; or account, credit card or debit card number in combination with any required security code or password that would permit access to an individual's financial account. This rather restrictive approach is believed to produce better results when it comes to the notification procedure since it avoids over-notification [Retzer 2008]. In any case, this issue is about to be determined by the national legislations that will implement the Directive.

## Field of Application

According to the new provision of the Directive, article 3 of the Directive 2002/58/EC is replaced by the following provision.

"This Directive shall apply 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."

It is clearly stated that the provisions of the Directive apply to providers of "publicly available electronic communications services". The term is defined in Directive 2002/2/EC as "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising edito-

rial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

Thus, the Directive applies to providers of public electronic communications networks and services (PPECS) i.e. telecom operators, mobile phone communication service providers, internet access providers, providers of the transmission of digital TV content" [Dhont, WoodcocK 2010].

In the preamble of the Directive (Recital 55) it is stated that the Directive "does not apply to closed user groups and corporate networks." However this is a point which lacks further clarification and it might be interpreted in many different ways .

As the Article 29 Working Party notices in its 2/2008 opinion it is not always easy to distinguish public service from a private one.

For example how can we reach the correct definition when internet access is provided by a multinational company to 300.000 employees? Should it be treated differently if it is provided by a cybercafé?

Since this point has been debated a lot during the whole procedure it is important to note, that the Article 29 Working Party and the European Data Protection Supervisor have proposed a broader application of the notification regime which should also include providers of information society services such as on-line banks, on-line businesses, on-line providers of health care services etc.

Especially in its second opinion the EDPS stresses that there are two reasons why the application of the notification procedures should be extended to Information Society Service Providers (ISSP's) Firstly by setting the example, of United States where almost all of the States have enacted laws on security breach notification "which have a wider scope of application, encompassing not only PPECS but any entity holding the required personal data." Second, by underlying that is not just personal data processed by PPECS that maybe breached, but all the types of personal and highly confidential information processed by ISSPs (i.e bank accounts, health-related information) could easily be disclosed, thus enabling the use for identity theft purposes [EDPS 2008].

Directive 2009/136/EC has a two-fold approach on this issue. The European legislature expresses is expressing a clear opinion on the preamble of the Directive supporting the expansion of notification requirements, as the "interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority" [Directive 2009/136/EC]. It is evident that even though this is not expressed in the word-

ing of the main text, it still has a particular importance and might be seen as an encouragement of the Member States, towards the extension of the notification requirements to Information Society Service Providers (ISSP's), when they implement the provisions of the Directive.

## Notification obligations

The European legislature added three new paragraphs to article 4 of the Directive 2002/58/EC. The new provisions that are added to article 4 provide that in the case of a personal data breach, a notification must be made to the competent authorities, subscribers and other affected individuals.

In particular, the Directive requires that the providers of publicly available electronic communications services, without undue delay, should notify the personal data breach to the competent national authority. This will have to be done irrespective of their possible harm [Van Quatherm 2010].

In addition when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider should also notify the subscriber or individual of the breach without undue delay. This is particularly important since if a data breach is not addressed in an adequate and timely manner, this could result in substantial economic loss and social harm, including identity fraud, to the subscriber or individual concerned [2009/136/EC Bottis 2010].

It should also be noted though that according to this provision if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so [Directive 2009/136/EC]. This provision clearly provides that data breach should be notified not only to subscribers but also to other entities.

Individuals affected by a certain data breach· this raises concerns over how this would work in practice since the service providers usually only have contact details of their subscribers . Of course it is possible that the intention of the Directive is to "cover users of ECSs that are not "subscribers" but with whom the service provider does have contact, and thus can easily be contacted in case of a breach" [Van Quathem 2010].

## Content of the notification

The notification to the subscriber or individual should describe i) the nature of the personal data breach ii) the contact points where more information can be obtained iii) should recommend measures to mitigate the possible adverse effects of the personal data breach and finally iv) when the providers notify the data

breaches to the competent national authority they should also describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach [Directive 2009/136/EC].

## Exceptions

Nevertheless, the notification to a subscriber or individual concerned is not required if the provider has demonstrated that it has implemented appropriate technological protection measures and the measures were applied to the data concerned by the security breach.

It is stressed that the technological protection measures should ensure that "personal data can be accessed only by authorised personnel for legally authorised purposes, and that the personal data stored or transmitted, as well as the network and services, are protected thus rendering the data unintelligible to any person who is not authorised to access it [Directive 2009/136/EC].

## Competences of National Authorities

A new paragraph is also added regarding the competences of National Authorities. Under the new regime the competent national authorities can i) adopt guidelines ii) issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made and iii) they should also be able to audit whether providers have complied with their notification obligations under this paragraph, and impose appropriate sanctions in the event of a failure to do so [Directive 2009/136/EC].

In addition providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of the Directive [Directive 2009/136/EC].

National Authorities will not be left alone to control the function of the new notification regime, since in order to ensure consistency in implementation of the provisions of the Directive, the Commission may, following consultation with the European Network and Information Security Agency (ENISA), the Article 29 Working Party and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements[Directive 2009/136/EC].

## *Tracking technologies*

Directive 2002/58/EC required Member States to implement restrictions on the use of hidden identifiers to ''trace the activities of the user'' on electronic com-

munication networks acknowledging that devices such as cookies, "can be a legitimate and useful tool, for example, in analyzing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions" as long as users were provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices and had the opportunity to refuse to have a cookie or similar device stored on their terminal equipment.

These provisions of the e-Privacy Directive were largely welcomed; "it was seen to legalize the use of cookies while providing a degree of consumer protection against hidden tracking" [Brunger, Watts 2010].

The new provisions of the e-Privacy Directive require websites to seek consent before placing "cookies" and similar devices such as spyware (hidden espionage programs) and Trojan horses (programs hidden in messages or in other software), on a user's computer.

In particular article 5(3) of the Directive 2002/58/EC is replaced. The Directive adopts the "opt in" approach on the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber. From now on, access and storing of information is only allowed· under 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·" In addition in the preamble of the Directive is it provided that the "user's consent to processing may be expressed by using the appropriate settings of a browser or other application."

The new provision offers exceptions to the "opt-in" regime, allowing the storage "where a cookie is necessary 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."

## Implications for on-line advertising

A number of serious questions have been raised in relation to the "opt-in" requirements. Marketers and advertisers are particularly worrying on the effect that the new provisions might have on their business. A number of questions have been raised in accordance to the implementation of these provisions. The first question dealt with the acceptance of the consent of the subscribers and users. Should each website have a certain page in which it provides information about its cookies? Should websites offer consent for each cookie, or each type of cookie used by the website? How should recital 66 of the preamble of the Directive be interpreted "The methods of providing information and offering the right to refuse should be

as user-friendly as possible"). Does this means that the "opt - out "regime still is in force and "if this is the case, then what is the difference with the current state, and what did the amendment intend to accomplish [itlawgroup].

In 2010, the Article 29 WP adopted Opinion 2/2010 on the online behavioural advertising attempting to clarify the new provisions of the amended e-privacy Directive concerning the placing of cookies and other tracking devices.

The Opinion notes that advertising network providers should firstly obtain informed consent before the placing of cookies or similar devices. Second, consent must be obtained only after prior informating about the sending and purposes of the cookie has been given to the user. Third, consent "must be, freely given, specific and must constitute an informed indication of the data subject's wishes". Fourth, consent must be revocable [Article 29 WP 2010]. Furthermore in the Opinion the Article 29 WP requires from advertising network providers to create prior opt-in mechanisms such as "browsers or other applications which by default reject third party cookies and which require the data subject to engage in an affirmative action to accept both the setting of and continued transmission of information contained in cookies by specific web sites ....." and the conveyance of "clear, comprehensive and fully visible information in order to ensure that consent is fully informed". This can only be done if "the browsers convey, on behalf of the ad network provider, the relevant information about the purposes of the cookies and the further processing". The Article 29 WP considers that users' single acceptance to receive a cookie could also entail their acceptance for the subsequent readings of the cookie, and hence for the monitoring of their internet browsing. Thus, to meet the requirements of Article 5(3) it would not be necessary to request consent for each reading of the cookie [29 WP 29 2010].

As stated above on-line advertisers and Marketers are particularly worried with the new provisions concerning cookies and expect the implementation at national level to see how the new e-Privacy Directive will finally be implemented. A fear exists that if the Directive is implemented based on the wording of the main text, that will probably have negative consequences for free internet services such as Facebook, YouTube and Spotify that "rely on the revenue generated from online advertising space" [Brunger Watts 2010] as this will annul anonymous tracking of users habits.

In response to the 2/2010 Opinion it has been noted that an overly strict interpretation of the e-privacy directive, would kill any chance of the media building viable advertising revenues online and our serious efforts to give consumers effective control over the use of cookies The Internet in Europe would become less attractive to users, something that would significantly undermine the growth potential of the digital economy and jeopardize the existence of European on-

line companies finally calling into "question the EU's ambitious Digital Agenda, intended to increase Europeans access to ultra fast Internet and fostering the e-commerce sector" [WFA 2010].

Still, as stated in the preamble of the Directive 2002/58/EC, "terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned". In addition, the basic internet technology allows ad-network providers to easily track data subjects across different websites and over time, they gather and analyze their surfing behaviour in order to build extensive profiles about data subjects' interests.

The profiles that have been gathered are able to single out internet users and potentially harm their privacy [Bottis 2010].

### *Unsolicited Marketing Communications*

In addition to the provisions regulating the use of cookies, the new e-privacy Directive amends article 13 of the Directive 2002/58/EC extending the scope of the Directive. Member States should provide that unsolicited commercial messages may be sent to subscribers and users unless they have previously opted-in to receive the message.

In particular, the Directive stipulates that "the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent."

The wording of Article 13.1 makes the assumption that the person is already connected to the network on which the communication is conveyed. It does not cover cases "where a solicitation would ask a user to connect to a network that serves advertisements exclusively. This may typically be the case in Bluetooth marketing applications" [WP 29 opinion 2009].

This observation has been taken into account in the preamble of the Directive is stated that "safeguards provided for subscribers against intrusion into their privacy by unsolicited communications for direct marketing purposes by means of

electronic mail should also be applicable to SMS, MMS and other kinds of similar applications" ensuring that prior consent is required in Bluetooth marketing applications.

However, a natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that i) the contact details are obtained from the customers in the context of the sale of a product or a service, ii) the contact information must be obtained in accordance with Directive 95/46/EC iii) the customers "clearly and distinctly are given the opportunity to object, free of charge and in an easy manner" iv) the customers are given the opportunity to object at the time of their collection and on the occasion of each message in case the customer has not initially refused such use.

At the end of the amended article 13(6) of the e-privacy Directive states that any natural or legal persons that have been adversely affected by infringements of national provisions adopted pursuant to the new Directive provisions, have the right to bring legal proceedings in respect of such infringements in order for them to seek the cessation or prohibition of such infringements. This new provision it has been seen as an important step towards the protection of both natural legal persons (such as consumer associations and trade unions representing the interest of spammed consumers) and PPECS against spammers since it allows Internet access providers to tackle spammers for abusing their networks, to sue entities counterfeiting sender addresses or hacking servers for use as spam relays [EDPS 2008], and thus defend the interests of their customers, as part of their own legitimate business interests [Directive 2009/136/EC].

## Conclusions

The introduction of the new amended provisions of the Directive 2001/58/EC is definitely the right step towards the strengthening of the personal data protection. Data breach notifications, expansion of the "opt-in" system regarding the acceptance of cookies and similar devices, anti-spam provisions and the right to bring legal proceedings against spammers, all form a "security-shield" necessary to protect consumer privacy and the development of on-line transactions.

The data breach problem is a rather complex which problem crosses all sectors. There is much more to be done and this issue should not be addressed only in the Framework of electronic communications. As it is stated in paragraph 59 of Directive 2009/136/EC, "pending a review to be carried out by the Commission of all relevant Community legislation in this field, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application throughout the Community of the

principles embodied in the data breach notification rules contained in Directive 2002/58/EC regardless of the sector, or the type, of data concerned."

The regulation of tracking technologies (spam and similar devices) raises important concerns amongst advertisers since it affects their ability to receive feedback on consumers browsing history making difficult targeted and behavioural advertising.

In relation to unsolicited electronic marketing communications protection includes not only users but subscribers as well. Moreover, it is the opt-in system in relation to unsolicited marketing communications sent via communications system is instituted by the Directive.

As stated above, the amended Directive is definitely a step towards the right direction but it might not be enough.

As electronic communications become more and more complex, consumers become more aware about their privacy. But privacy concerns might lead to a diminished use of Internet transactions and subsequently to a loss of revenue for e-commerce.

Therefore companies and internet providers should invest on security technology since in an environment of technology, the answer to privacy problems cannot be regulation alone.

## References

Brunger James, Watts Mark " Changes to the European E-Privacy Directive, Consequences for Online Advertising" http://www.bristows.com-/?pid-=46&nid=1494&level=2 (The article was first published in the Privacy & Security Law Report by The Bureau of National Affairs, Inc.) (accessed 12.5.2010)

Bottis M., Cate Fred (2008), "Information Security Breaches: Looking Back & Thinking Ahead" The Centre for Information Policy Leadership http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf.(accessed on 11.6.2010)

Clifton Phua (2009) "Protecting organisations from personal data breaches" Computer Fraud & Security, Pages 13-18

Commission Nationale de l'Informatique et des Libertés (2002) "Opération 'Boîte à spams': Les enseignements et les actions de la CNIL en matière de communications électroniques non sollicitées," report submitted by Ms. Cécile Alvergnat and adopted 24 October 2002. http://www.cnil.fr/fileadmin/documents/approfondir/rapports/boite_a_spam.pdf (accessed on 1.6.2010)

Cooper Dan, Fink David, Jones Emile, Van Quathem Kristof (2006). "Security Breach Notification in Europe on The Orizon" World Data Protection Report, 10/06 http://www.cov.com/files/Publication/69e65c7e-4d08-474e-853-b-3635e9120777/Presentation/PublicationAttachment/4064434a-7a6e-419e-89963c810d88da9c/757.pdf (accessed on 1.6.2010)

Dhont Jan, Woodcock Katherine (2010) "New Security Breach Notification Requirements Under Amended E-Privacy Directive" http://www.lorenz-law.com/wp-content/uploads/021-Notification-requirements-under-amended-E-Privacy-Directive-19012010.pdf (accessed on 1.6.2010)

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

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*

Finklea Kristin (2010) "Identity Theft: Trends and Issues" Congressional Research Service Report 1/2010, http://assets.opencrs.com/rpts/R40599_20100105.pdf(accessed on 1.6.2010)

Gauthronet Serge Drouard Etienne (2001) "Unsolicited Commercial Communications and Data Protection" (Internal Market DG – Contract n° ETD/99/B5-3000/E/96) January 2001, Commission of the European Communities http://www.rigacci.org/docs/biblio/online/spam_garante/document/434683.pdf (accessed on 1.6.2010

Gindin Susan (1997). "Lost and Found in Cyberspace-Informational Privacy in the Age of the Internet" 34 San Diego Law Review 1153

It Law Group (2010),"What's Cookin' in the European Union?" http://www.itlawgroup.com/index.php/resources/publications/169-of-cookies-and-spam?format=pdf (accesed 30.5.2010)

King Ian (2003) "On-line privacy in Europe—new regulation for cookies" , Information & Communications Technology Law, Volume 12, Issue 3 October 2003, pages 225 - 236

Maurushat Alana (2009) "*Data Breach Notification Law Across the World from California to Australia*" (accessed on 11.6.2010)

Mitrakas Andreas (2006) "Information security and law in Europe: Risks checked?" Information & Communications Technology Law, Volume 15, Issue 1 March 2006, pages 33 – 53

Munir Abu Bakar, Privacy and Data Protection:
International and Regional Instruments 20th BILETA Conference: Over-Commoditised; Over-Centralised;Over-Observed: the New Digital Legal World? Lexis-Nexis (2005)

Opinion 2/2010 on online behavioral advertising, Article 29 WP ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp171_en.pdf

Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) Article 29 WP http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_en.pdf

Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive) http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_en.pdf

Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications (2008/C 181/01) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_EN.pdf

Poullet Yves "Data protection legislation: What is at stake for our society and democracy? Computer Law & Security Review 25 (2009) 211 – 226

Romanosky Sasha, Telang Rahul, Acquisti Alessandro (2008) Do Data Breach Disclosure Laws Reduce Identity Theft? Seventh Workshop on the Economics of Information Security, June, 2008. http://weis2008.econinfosec.org/papers/Romanosky.pdf. (accessed on 1.6.2010

Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2009/C 128/04) point 19

Solove Daniel (2004) "The digital person: technology and privacy in the information age", http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text/Digital-Person-CH2.pdf (accessed on 1.6.2010)

Turle Marcus (2009) “Data security: Past, present and future” Computer Law & Security Report, Volume 25, Issue 1, 2009, Pages 51-58

Van Quatherm Kristof (2010) . “Security breach notification in the European Union: First step taken, more to come” 01/10 World Data Protection Report BNA http://www.cov.com/files/Publication/3c4eadcd-c074-44f8-925f-4a63d5304d70/Presentation/PublicationAttachment/9c8fb8a0-b55a-4464-ac4b-4a7722e-da833/Security%20breach%20Notigication%20in%20the%20EU%2c%20first%20step%20taken%2c%20more%20to%20come.pdf (accessed 11.6.2010)

World Federation of Advertisers (2010) http://www.wfanet.org/press_releases.cfm (accessed on 1.6.2010)

# Some thoughts on the moral foundation of the intellectual property rights

**Lambros Kotsiris**

Law has been associated with written words. 'The Law' was for the Jewish people their sacred book. Spoken language was supplemented by writing without being displaced. Wittgestein has written that man has the ability to construct languages by which man expresses what each word means-language translates thought (Tractatus Logico-philosophicus). The distinctiveness of law in language, as well as its method and material, are traits its autonomy in the modern world, a mystified social structure, unknown to those not trained in law. Legal normativity withdraws behind the veil of expertise. But the information technology, on the one side, threatens to increase the distance when it requires technical competence; on the other side, it allows the impenetrability and the accessibility to knowledge. Social organization, due to the velocity of information, becomes more flexible and self-actualized, beyond the horizon of the mystified legal order.

Today, we have passed from using stable knowledge, as the foundation of any activity, to a continuous education and familiarization with a kind of knowledge now in the center of our attention. Once, knowledge used to be at the bottom; now, knowledge appears at the surface, and has a constantly moving form, supporting every action. Information and knowledge have become the most important economic goods. Unlike the teachings of the classical economy, knowledge and information are governed by two laws: first, their consumption or use does not destroy them and second, their transfer means no loss. For the rest, the word belongs to the experts, as "for those about one cannot talk, one must remain silent".

'Foundation' has two, main, meanings: 1. What gives to a thing its existence or the reason of its existence, what legitimates the consent of my spirit for an affirmation and 2. a general clause out of which we may produce a whole totality of knowledge and definitions. 'Foundations have been for a long time synonymous with abstract buttress. Later, they signify whether general principles on which a metaphysical system can be based on the specific principles, on which a particular science is based or the justifying/supporting facts. Now, the discussion about the moral foundations of law must address the question whether legal principles must ever operate as legal norms. This matter has become, these last years, the subject of an extensive debate among legal positivists. Three positions have

emerged: a. The consistency of a norm with some or all requirements of morality is a precondition for the status of this norm as a legal rule in a particular jurisdiction (inclusive legal positivism). This consistency, as a precondition of legal validity, is not inherent in the concept of law. It is, instead, a kind of a threshold test under the unwritten rule of recognition in a legal regime, a feature only contingent, rather than essential, of the system of law in which this test is applied. 2. Under the 'incorporation theory', a norm's correctness as a moral principle is a sufficient condition for its status as a legal norm in a given legal order. Even for the "incorporatists", the incorporation of moral principles in a legal system is only contingent rather than inevitable. 3. Exclusive legal positivism is opposed to the first two positions described here. It maintains that the very nature of law is inconsistent with the role of moral principles as legal norms or as standards for the validity of legal norms.

Apart from these three theories, the 'value doctrine' maintains that the law is a morally valuable institution as a part of nature. "Being valuable" is a moral property, which the law enjoys due to its nature, as law realizes valuable ends, performs as institution, moral tasks and in itself is a valuable institution.

The law as part of culture is value-connected (Radbruch). The law is the reality which serves justice. This concept of law is not positivism. Positivism understands law as the totality of norms of any content. The "value" theory emphasizes that only norms serving justice are valuable. This is, also, not natural law, as the 'right' law is not identified as having the absolute value of justice.

In the end, we must agree with the philosopher Kaufmann that legal jurisprudence is dominated today by the confession that we don't know what law is. This is a reflection of a deeply-rooted perplexity about what we really are. If I am not mistaken, Dostoyevsky once noted that ants know how to gather their food; bees know how to build their beehive; only man does not know his formula.

As in other areas of law (contract law, public law etc) we address today questions on the moral foundations of intellectual property. It is exactly the topic of the congress which pushes intellectual property to the room of doubts. In the era of a technological world, Professor Ginsburg, referring to intellectual property, writes that there is nothing 'sacred' in relation to the ideas of the 18$^{th}$ century for a world which, at that time, could not even be imagined. Information becomes knowledge-to knowledge, everyone must have free access. A new world order had emerged, a general dynamic of the so-called virtual reality.

In that scenery, economic theory enters. Unlike other woods, works of art, literature, science, technique may be employed by millions of people without being consumed. They remain intact. Therefore, the marginal cost of their dissemina-

tion to the public in a material or electronic form is nearly zero. Even the extremist social philosopher Pierre Proudhon in his writings, in the midst of the 19th century (Les majorats litteraires) looks at the works of authors as simple products brought to the market, asking for an exchange. Creation of works means production by transformation of materials, exactly as the one of the merchants and the bankers. Proudhon does speak about property but more precisely, about a time-limited privilege, for sale. He adds: any work of authorship is exactly as man: incomplete, temporary and capable for services for a limited time. Hardin in his famous book 'the tragedy of the commons', where any additional animal in a limited space endangers the existence of all, maintains that the greater the number of people who participate in knowledge, the richer the productive space. From this space, authors 'pump' themselves, therefore they owe to it. Another American theorist, Netanel, conemns the expansion of copyright, because it imposes an unacceptable burden on the values of free speech. Any approach to material is here not to be found. Even the recent approval of the idea of property as a stable and despotic dominion (property essentialism) while the reasons underlying a property right remains irrelevant, does not give a link to morality. The core of a property right is the exclusion of any third party (exclusivity axiom). The theory of incentives in favor of intellectual property goes back to Adam Smith and natural law. It looks at the protection of intellectual property as the necessary incentive for intellectual production and at the same time, as the means for the exclusion of any unauthorized used of intellectual creations. The new classical economic theory acknowledges that intellectual property protection is not only an incentive but even a mechanism facilitating market allocation of the works of the author.

Where are the moral foundations of an intellectual property right to be found? The easiest way is to refer to the personality, as a complex frame, and all the kind of properties arising out of it. In the preamble of the 1791 French Copyright Act, we read that the most sacred, unviolable and personal of all the properties is the work, product of the author's mind. Even the founders of this Act had therefore spoken about "property"-this justifies the author of a work to say "what I have created belongs to me". Rousseau in his Essay "on the origins of inequality of men' writes that the first man who put a fence around a piece of land and said "this is mine" while other men believed him and accepted this, was the founder of civil society and the concept of private property.

The predominant answer to the question about the moral foundation of intellectual property is given by John Locke. For him, every man, by the laws of nature, enjoys a right to his life, his freedom and his goods. Every man dominates his own person. Everyone carries in her own self the foundation of property. Given that man is master and owner of herself, she is the owner of her labor of the efforts of her body and the work of her hands. Whatsoever then she removes from

nature and mixed with his own labor is something that is her own, her property, under the reservation that at least enough and as good left is common, remains for other people. For Locke, man expands her ego since working on objects transmits to them something of his existence.

Morality for the Socratic philosophy is not inherent in us; it can be learnt. It is connected with education. Close to this idea is the theory of democratic paradigm. Intellectual property is considered to play a central role for the progress, education differentiation and expression. In a pluralistic society, intellectual property is a factor of a progressive democratic governance. It has a core role for the democratic character of public dialogue and the freedom of intellectual production. At the same time, intellectual production frees creation from the state dominance and censorship. Thus, intellectual property is incorporated in the social sphere of communication. The problem is everlasting, both philosophical and social and difficult to resolve. Philosophy understood whether as teaching or, with Wittgestein, as activity, which clarifies and delimits strictly the thoughts, begins when philosophic thought has done its best and the wonder remains. Besides, this is the best possession of the human spirit (Alfred Whitehead).

# The potential of e-justice in Brazil

**Cláudio S. de Lucena Neto &**
**Antônio Silveira Neto**

## Introduction

Access to justice, the guarantee offered by the State that a violation of one's rights will be taken before – and these rights eventually secured by – a judge, or a court of justice is a fundamental human right for a society that intends to provide its citizens with a modern and egalitarian legal system. A menace to this fundamental right of reaching the judiciary system whenever necessary is a menace to the essence of the society itself.

## Access to justice in Brazil

The Brazilian legal system is organized in such a way as to suggest that this broad access stretches out to a practically unlimited extension. This so-called universal access to justice is implemented through diverse mechanisms. Gratuity of access to a lawsuit is constitutionally secured to any Brazilian citizen or resident who proves unable to afford the costs of the demand, including applicable expenses and taxes, technical production of evidence, and even lawyers' fees. Television advertising, informing the population what and where are the legal services available to people have also become a popular strategy trying to minimize the distance between courts and citizens. A television channel, with extensive internet interaction, exclusively dedicated to cover news, information and decisions related to Brazilian legal system is on the air, nationwide. Even a strong movement of simplification of the legal jargon in Brazil is on the move. All of these actions, from the development of legal tools in the Procedural Law system, to more generic Justice administration policies, reveal a clear tendency of bringing the judiciary power in Brazil much closer to the citizen than it used to be in the previous decades.

## The social costs of a wide open access to justice

Guaranteeing this access, however, can bring its own and often demanding challenges. The population in Brazil has reached approximately 190 million people. A country with continental dimensions obviously has to face continental-size problems. As a result of these wide open access to justice, Brazilian courts hear over

nothing less than 45 million lawsuits, with 18,6 million new lawsuits filed every year, before different instances of the judiciary system. It is a massive problem to be faced, where creativity and innovation are necessary, but also confronted and frequently limited by legal parameters of procedural law, and constitutional guarantees.

This enormous amount of lawsuits is certainly one, if not the main reason for the excessive amount of time that it takes a legal solution to be found in a case presented before a Brazilian court of justice. No matter the number of judges working in the country, the proportion of judges per case will hardly ever be ideal in this scenario. It also believed that such a broad access to justice may also have contributed to a high degree of litigiousness which can be found in Brazilian society. The Brazilian State of Rio Grande do Sul, for example, led the statistics of lawsuits filed in 2008, when 1,5 million new cases reached the State Court, in a proportion of more than 14 new lawsuits per 100 inhabitants.

It is imperative that Brazilian society finds a way to deal with these problems and, principally, with its consequences. A proper solution can never depend upon a single policy, measure, law or decision. An adequate approach to face the unwanted effect of the excessive duration of a lawsuit in Brazil has to consider different factors, variables, characteristics and – perhaps the most important – start from the understanding that it is the model of justice administration adopted in the country, rather than the forms that surround it, that creates the conditions for these issues to arise.

## Justice productivity and the guarantee to reasonable duration of a lawsuit

The history of lawsuits in Brazil is one of patience, paper and time. Due to historical reasons and influences, the country has a tradition of written, excessively formal and solemn legal procedures, some of which end up compromising effectiveness, and the reasonable expectation of the citizen – which, in Brazil, has achieved the status of a constitutional right – that the intervention of a Judge, in the role of the State, will actually find and dictate a solution for his problem. Theorists refer to this as the principle of the reasonable duration of a lawsuit. This way of understanding a lawsuit transformed it in an aim, an objective, rather than in a tool to achieve a greater goal, which should always be the solution of social conflicts and controversies, with only the formalities that are essential to keep the integrity and stability of the procedural system. Brazilian society has always lived with lawsuits which were excessively formal and lasted excessively long. A lawsuit that disregards essential, legal material issues to dedicate itself to

sheer procedures, or that lasts indefinitely in time is of little or of no use at all as long as effective justice is concerned.

As courts get closer to the public, and the citizen finds more and more democratic tools to access the Judiciary system, the number of lawsuits grows, what leads to other complications, as, for example, extremely high costs to keep the structure always functional and available, and at least one objective, operational problem of storage of these records.

The duration issue may be faced in many ways. Mediation and arbitration experiences have been conducted in the country, in an effort to reduce formal litigiousness and abbreviate conflicts. Procedural law is in constant change, the latest amendments concerning enforcing decisions of first instance and protective and precautionary measures which are necessary to secure the effectiveness of the legal action, as well as attempts to reduce technical options to appeal and bring discussions to higher courts, all of these as mechanisms to reduce delay. Productivity aims have been established, the last one requiring judges prioritize and decide actions filed before 2005. These are not pioneer actions. The State of California passed the Trial Court Delay Reduction Act, in 1992, systematizing official actions to eliminate delay in the progress and ultimate resolution of litigation, as an evidence that efforts to assume and maintain control over the pace of litigation is a worldwide concern.

## Information technology resources serving the administration of justice

Recent years have brought new perspectives in the efforts to find a solution to the aforementioned problems. The alternative which is the object of this work is, in fact, nothing more than a new perspective in justice administration. New tools, based in instruments provided by information technology, that offer one more alternative to achieve the goal of effectiveness, and whose first implementation results already show a strong indication that it can be a valuable mechanism for the cause.

Software and integrated systems which makes it possible for information technology to help store and conduct a lawsuit through electronic records and communication have been discussed and tested in Brazil over the last decade. After some isolated experiences, in 2006, a federal law went into force (Federal Law n.° 11.419/2006), allowing Brazilian courts to implement digital procedural systems and solutions. The country is nowadays promoting an institutional approach as part of the effort to face the historical problems faced various institutions in Brazil, such as universities, lawyers' associations and research institutes have decided to take part in the quest and walk this step forward in facing the problem.

Led by the Judiciary, through practical initiatives proposed and conducted by the National Council of Justice, the change is going on.

It is important to stress that the way lawsuits are being migrated to digital media in Brazil does not imply significant change to the structure of national Procedural Law, but a simple innovation in the model. Having discovered that 60% of the time of a lawsuit consists of pure bureaucratic activities, what happens is that these bureaucratic procedures are considerably spread through massive use of IT resources, with minimum legislative effort, eliminating redundant work, and allowing some tasks to be automated.

## E-process tools and systems

Paper is eliminated, the systems receive digitally certificated files as legal documents, communication and notification of the events of the case is carried out through the Internet, and the final command is also often fulfilled by electronic means. Records are also kept and accessed by electronic means, dismissing the physical existence of the lawsuit, at least in paper form. Results are only starting to arise, but are already stimulating.

Although the systems currently in use just reproduce the model of an ordinary paper lawsuit, the mere use of a structured computer system to organize a legal action manages to eliminate, as already said, redundant, repetitive work, extinguishing some useless, time-consuming bureaucratic-only tasks, speeding the whole process, results suggest. In addition, these systems provide the extremely useful alternative to automatically store precise statistic data that can be further used to monitor and feedback the system, for decision-support purposes.

According to the Labor Court of the State of Paraíba, one of the pioneer instances of Brazilian justice to adopt and implement electronic lawsuit systems and tools, the time reduction effect could be perfectly noticed in the very first year of the experience. In may 2009, after a year of operation of the system, some time lapses, as the time to schedule a hearing, conclusion of the case to a decision, and execution of the decision itself have decreased an average of 50%.

## Conclusion

The results, as has been pointed out, are still preliminary. Although they can be exciting, since it is a simple conceptual innovation that can bring positive impacts in the productivity of Brazilian justice, further investigation has to monitor and continuously analyze the middle and long term effects of the large scale implementation of this solution, to verify if similar results will be achieved in different

spheres of the judiciary power, like civil, administrative, taxation, criminal, constitutional, electoral and other courts of justice.

Finally, it is also essential to deepen the study to evaluate to what extent the historical problems of duration, formality and storage can be adequately faced with minimum side effects, and minimum impact on other complex issues, such as privacy, security, and accessibility.

## References

Conselho Nacional de Justiça. A Justiça em Números – Dados Estatísticos do Judiciário Brasileiro, http://www.cnj.jus.br

California Government Code Sections 68600-68620. Trial Court Delay Reduction Act, http://law.justia.com/california/codes/gov/68600-68620.html (31/01/2010).

Cappelletti, Mauro & Garth, Bryant. Acesso à justiça. Translated by Ellen Gracie Northfleet. Porto Alegre: Fabris, 2002.

Cardozo, Benjamin N. The Nature of the Judicial Process, New Haven: Yale University Press, 1921.

Bielsa, Rafael A. & Graña, Eduardo R. El tiempo y el proceso. http://www.argenjus.org.ar/argenjus/articulos/granabielsa.pdf (15/12/2009).

Brasil. Lei 11.419/06. Dispõe sobre a informatização do processo judicial; altera a Lei no 5.869, de 11 de Janeiro de 1973 – Código de Processo Civil; e dá outras providências http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm (20/12/2009).

Garcia, Sérgio Renato Tejada. Processo virtual: uma solução revolucionária para a morosidade. http://www.cnj.jus.br/index.php?option=com_content&view=article&id=50:processo-virtual-uma-solu-revoluciona-para-amorosidade&catid=74:artigos&Itemid=129 (10/01/2010).

Lima, George Marmelstein. E- processo: uma verdadeira revolução procedimental. http://jus2.uol.com.br/doutrina/texto.asp?id=3924&p=1 (13/08/2009).

TRT 13ª Regiao. Vara Eletrônica completa um ano e prazo de julgamento cai para 12 dias. http://www.trt13.jus.br/engine/interna.php?pag=exibeNoticia&codNot=1429 (31/01/2010).

# The electronic communications regulatory framework & the internal market - the spectrum policy case study

**Marina Markellou**

The existing regulatory framework for electronic communications networks and services comprises five directives, together referred to as "the Framework Directive and the Specific Directives"[2]:

- Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to electronic communications networks and associated facilities
- Directive 2002/20/EC on the authorization of electronic communications networks and services
- Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services
- Directive 2002/22/EC Universal Service Directive and
- Directive 2002/58/EC Directive on Privacy and electronic communications. This legal Framework regulates all electronic networks and communications services that are transmitted electronically, whether fixed or wireless, data or voice, Internet-based or circuit switched, broadcast or personal.

The European Commission is positive about the progress made since 2002 in opening up national telecoms markets to competition. The main goal of this regulation is to create and complete the internal market for electronic communications by strengthening the Community mechanism for regulating operators with significant market power in the key markets. The establishment of an internal market for electronic communications is a topic of high priority because of the increasing economic importance of the telecoms sector in Europe[3].

But what is actually an internal market? The development of an internal market is one of the rationale of European intervention and the main objective of electronic communications regulation. Indeed, achieving the Internal Market in the communications sector is of strategic significance for the Europe not just because communications as such is one of the leading sectors of the European economy but also because the whole of economy benefits from a healthy and efficient commu-

nications sector. We remind that the ambitious objective of The Lisbon European Council for Europe was to become the most competitive and dynamic knowledge based economy in the world, capable of sustainable growth with more and better jobs and greater social cohesion. It is not sufficient to make the national markets more competitive they must also be more integrated.

The European regulatory framework for E-communications networks and services should therefore be reformed in order to achieve a single European market for telecoms. On 24 November 2009 the European Parliament at its plenary session in Strasbourg formally approved the European Telecoms Reform Package after two years of discussions[4]. Three are the main parts of the package: the E-coms framework directive, the citizen's rights directive and the establishment of a new Body of European Regulators for E-coms (BEREC). The reformed Package entered into force with its publication in the Official Journal of the EU on 18 December 2009. The 17 Member States have till July 2011 to transpose these new rules into their national telecommunication laws. BEREC was established in January 2010[5]. BEREC unites the national telecoms regulators of the EU Member States and seeks to strengthen the EU telecoms market and guarantee fair competition. BEREC replaces the European Regulators Group (ERG), the previous organization within which National Regulatory Authorities (NRA's) exchanged their expertise and thoughts on the functioning of the telecoms market in the EU. BEREC provides a forum for the regulators to coordinate pan-European policies and study new developments in the telecoms market. BEREC will provide opinions, reports and advice to the National Regulatory Authorities, the Commission and, on request, to the EU Parliament and the Council.

The Review of the European regulatory Framework for Electronic Communications aims to ensure that the framework continues to serve the needs of the next decade. In that regard, the review aims to diminish the regulatory fragmentation and inconsistencies between the activities of the national regulatory authorities in order to reinforce the competitiveness of the sector and the substantial consumer benefits from cross-border competition.

The Procedure for the consistent application of remedies is described in article 7a of the Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009. The National Regulatory Authorities shall contribute to the development of the internal market by working with each other, the BEREC and the Commission in a transparent manner. Under the procedure of article 7, the national telecommunications regulators must submit their market analyses and their regulatory measures to the Commission before adopting final decisions with a view to consolidating the internal telecoms market. The European Commission can raise serious doubts about the draft measure that a National Regulatory

Authority intends to take - if BEREC agrees, the National Regulatory Authority amends or withdraws - if not, the National Regulatory Authority provides serious justification - in all cases the European Commission recommends.

The Telecom package reform clearly proves that the establishment of an internal market for E-Communications is a topic of high priority. A European Commission report released on 1 June 2010 shows that EU telecoms markets have become more competitive thanks to the Commissions guidance in the consultation and review process known as the article 7 procedure[6].

Despite of the fact that all the previous measures were taken, one important question is raised: have we got a full market for Electronic Communications? A single European telecommunications market is still far from reality. An example that reflects this consideration is the Radio Spectrum Case study.

The radio spectrum is defined as all the waves operating at frequencies between 3 KHz and 300 GHz. It is divided into "bands", i.e. ranges of frequencies. Different applications use different bands: terrestrial TV is between 400 and 800 MHz, mobile phones around 900,1800 and 2000 MHz, cordless phones below 1900 MHz, Wifi "hots-spots" at 2.4 or 5 GHz and satellite communications often at even higher frequencies. The radio spectrum accommodates a growing number of applications (TV, mobiles, GPS, civil and military radars, earth observation and weather satellites, telemetry, radio astronomy, medical implants, hearing aids....)[7].

On the issue of radio spectrum, the Commission advocates moving towards a common, a more flexible and market-based approach for allocation of the radio spectrum needed for innovative services and for devices to work EU-wide. To accomplish that, the Commission intends to give spectrum usage right holders substantially more freedom to choose radio network and access technologies used (technology neutrality) as well as services offered (service neutrality)[8].

The strategy for flexible use of the Radio Spectrum can be briefly summarized as:

- Non exclusive use by a particular service, such as mobile or broadcasting.
- Non restrictive approach to the use of radio resources for electronic communications services.
- The scarcity of the resource requires judicious management: that means common definition of certain bands, easy and rapid transfer of spectrum, usage rights, and common European position for negotiations with third countries.
- No fragmentation that stops the innovation and the creation of a true single market.

By providing a structure for coordination and collaboration, the European Commission can enable Europe to take a single, strategic and coherent path towards spectrum reform.

De-regulated access to spectrum can encourage the development and use of innovative technologies and the Commission's strategy for promoting a flexible market also aims at creating new opportunities in existing allocations, e.g. spectrum formerly used for voice communications will become available for new broadband technologies which allow mobile Internet access.

Similarly, the Commission believes that a flexible approach should be taken when identifying parts of the radio spectrum for new uses. For example the transition from analogue to digital broadcasting will lead to a considerable spectrum 'dividend'[9].

The Commission services organized a public consultation until 9 April 2010 on the possible content of a proposal for a multiannual radio spectrum policy programme for the period 2010-2015.[10] The objective of this programme as stated in article 8(3) of the Framework Directive is to set out the policy orientations and objectives for the strategic planning and harmonization of the use of radio spectrum in accordance with the provisions of this Directive and the Specific Directives.

In line with this Directive, the up mentioned Programme will take the form of a legislative proposal by the Commission to be adopted by the Parliament and the Council. The Commission will also take into account the opinion of the Radio Spectrum Policy Group and on the results of the Spectrum Summit. The Radio Spectrum Policy Group was established under Commission Decision 2002/622/EC, amended in December 2009 and it gathers high-level governmental experts of the 27 EU member states[11].

The European Spectrum Summit has taken place in Brussels on 23 March 2010 and there was reaffirmed that spectrum should be accessible to innovative services and that the 800 MHz band will be soon a subject of a Commission decision. Neelie Kroes, the Vice-President of the European Commission and the Commissioner for the Digital Agenda mentioned the proposal of the adoption by the Commission of a technical harmonization on the 800MHz band which is one part of the digital dividend frequencies. This will set the technical conditions to apply in any Member State that decides to move away from using this sub band for broadcasting and will ensure a harmonized approach to the introduction of the Wireless broadband there. The Radio Spectrum Policy Group assured that coordinated availability of the 800MHz band for Electronic Communications Services other than broadcasting should be achieved in all EU Member States by 2015.

«I am not naïve – Mrs Kroes said - change may have an unsettling effect on some industries that are less prepared or less used to regular innovation. But, frankly, that is life. (...) When the world changes you have to change with it[12]».

## Endnotes

1. See http://europa.eu/legislation_summaries/internal_market/single_market_services/l24108i_en.htm.
2. See M. Cave and P. Larouche, "European Communications at the Crossroads", Report on the CEPS working party on electronic communications, October 2001.
3. See http://www.europarl.europa.eu/wps-europarl-internet/frd/vod/player?date=20091124&language.
4. See http://berec.europa.eu/.
5. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/644.
6. See: http://ec.europa.eu/information_society/policy/ecomm/radio_spectrum/_document_storage/videos/what_is_rs.swf.
7. See EBU's technical Review: "The terms "technological neutrality" and "service neutrality" are frequently used by regulators and particularly by the European Commission. The policy of "technological neutrality" is simple to explain: regulators should let the market decide which technology should be used for a particular purpose. "Service neutrality" is a more recent concept than technological neutrality – and slightly more difficult to define. In essence, it implies that regulators should encourage more flexible use of spectrum by allowing ANY frequency band to be used for ANY type of service". http://www.ebu.ch/en/technical/trev/trev_312-editorial.html.
8. See Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Rapid access to spectrum for wireless electronic communications services through more flexibility, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0050:FIN:EN:HTML.
9. See http://ec.europa.eu/information_society/policy/ecomm/radio_spectrum/rspp/index_en.htm.
10. See http://rspg.groups.eu.int/.
11. See Neelie Kroes, Why Europe needs effective co-ordination Spectrum Summit, European Parliament Brussels,23March2010 http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/115&format=HTML&aged=0&language=EN&guiLanguage=en.

# Privacy challenges and perspectives in Europe

Lilian Mitrou

## What are we talking about or visions of privacy

There are plenty of visions of informational privacy in literature, jurisprudence and legislation: the right to be let alone, the protection of the intimate sphere and information related to this sphere, the dignity approach are enriched by broader visions, which refer to privacy as freedom and informational self-determination or newer visions focusing on "identity" (Hildebrandt, 2006). However, it is not at all easy to define neither informational privacy nor the underlying interests: these interests range from autonomy, (informational) self-determination, balance and division of powers, over integrity and dignity, to democracy and pluralism (De Hert and Gutwirth, 2006). Continental European privacy protection regimes are, at their core, a form of protection of a right to respect and personal dignity. In this paper informational privacy is perceived not as informational seclusion but merely as a right, which enables individuals to exercise control over their own information, a prerequisite for being able to formulate conceptions of self, values, preferences, goals and to protect their life choices from public scrutiny and social disgrace.

This contribution refers to the challenges and perspectives of informational privacy, in other words to the present and future of privacy in Europe. The "end of privacy" is increasingly talked about. Is privacy "already dead" and we should "deal with it"?, as Scott McNally, the CEO of a large IT company has declared, or at least it is widely reported to have declared, some years ago? Are rumours of this death "greatly exaggerated" (Buttarelli, 2010a)? Does privacy remain a still valid constitutional value, a "necessary utopia" to use the words of Prof. S. Simitis? This paper deals with this critical question, by sketching out the regulatory context as well as the technological and legal challenges that politicians, legislators and last but not least, society have to face in relation to preservation of privacy in the new socio-political context.

## The European constitutional and regulatory framework

Under Article 8 of the European Convention on Human Rights (ECHR), "everyone has the right to respect for his private and family life, his home and his

correspondence". The European Court of Human Rights has perceived and construed Art. 8 broadly to protect individuals against the collection and processing of personal information, even if that information is considered banal or is already widely available. Fifty years later, the Charter of Fundamental Rights of the European Union adopted the distinction between the "right to respect for his or her private and family life and correspondence" (Article 7), which is modelled after the ECHR and "the right to the protection of personal data" (Article 8), which is consolidated thereby as a new, autonomous fundamental right. Moreover, Article 8 of the Charter lays down the components of this "new right", which at the same time constitute data processing criteria, i.e. fair processing, purpose limitation, consent of the data subject (De Hert and Gutwirth, 2006). The Charter expressly envisages access rights for individuals and provides that "compliance with these rules shall be subject to control by an independent authority". The right to respect for private life and the right to data protection remain however inevitably interrelated: Data protection regulation's main objective is to protect individuals against unlawful and unjustified collection, storage, use and dissemination of their personal data. This aim seems to be indebted to the central objective of the right of privacy even in its traditional approach, i.e. to protect individuals against unjustified interferences in personal life.

The right to data protection and – consequently - data protection regimes have gained significant importance under the Lisbon Treaty, as the Charter of Fundamental Rights of the European Union has become binding both on the Union and on the member states, when the latter implement European law. Another significant institutional change is that there is no more a pillar structure, which was characterized by remarkable differentiations of data protection's levels (Hustinx, 2010 a RISE). The current situation in the former third pillar can be described as a patchwork of data protection regimes. The Council Framework decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [Council Framework Decision 2008/977/JHA of 27 November 2008 Official Journal L 350, 30/12/2008 P. 0060 – 0071], even if strongly criticized, can be seen as a first step towards a more general framework (DPWP, 2009). Article 16 of the Treaty on the Functioning of the European Union was introduced as a new legal basis for data protection applicable to all processing in the area of police and judicial cooperation and common foreign and security policy, giving an a new institutional impulse to data protection.

With the general Data Protection Directive (Directive 95/46/CE) the European Union adopted a comprehensive regulatory model. The common legal framework for the 27 EU Member States is completed by the specific e-privacy Directive ( Directive 2002/58/CE). This framework is under revision: The European Com-

mission has some months ago launched a consultation regarding the amendment of the Data Protection Directive, while Directive 2009/136/EC has partially amended the e-privacy Directive. The EU's revised framework for electronic communications clarifies the responsibilities of network operators and service providers, including their obligation to notify breaches of personal data security. Undoubtly the European data protection framework has been the "result of political strive and compromise" (Burkert 2009). However and despite the problems concerning the transposition in Member States, the time after the adoption of the Directive and before 2001 could be regarded as "the Golden Age of Data Protection".

## Are the "heydays" over? A new balance or Europe as a surveillance society?

Privacy would appear to be doomed in the "age of terror". The suggestive powers of the images of the terrorist attacks of September 11th, 2001, a kind of a Doomsday of informational privacy, put the subject of "security" back on the political agenda with both a vengeance and a new accentuation. In the wake of each attack in Europe, earlier legislative proposals, which had "no chance to be accepted" (Hofmann-Riem, 2002, IPTS 2003), were re-introduced, and new policies with similar objectives were drafted to extend state surveillance authority (Mitrou, 2008).

Legislative activism was fuelled by the assumption that – despite the existence of information which might have presaged the terrorist attacks- the intelligence and law enforcement agencies were unable to "connect the dots" in such a way as to prevent these attacks (Taipale, 2004). After 9/11, many reference criteria changed and the guarantees were reduced everywhere in the world, as shown particularly by the Patriot Act in the USA and the European decisions on transfer of airline passenger data, the so-called PNR data to the US as well as on the retention of electronic communications data. Law enforcement and intelligence agencies have been eager to gain access to the wide range of personal information that has become available from information systems often created for very different purposes. The Council Decision on Prüm and its implementing decision, leading to the compulsory storage and exchange of DNA and fingerprinting data between the authorities of the Member States; the new legal frameworks for Europol and Eurojust, with additional possibilities for data use and exchange by these bodies are the most obvious examples of ever growing data sharing among Member States. The trends are visible: ubiquitous data availability, widespread and often excessive information sharing, and surveillance often via automated means that are inclined not only to errors but also to discriminatory effects (Buttarelli, 2010a).

Consequently, some of the principles underlying the system of personal data protection are being slowly but clearly eroded. This concerns, first and foremost, the purpose limitation principle as well as the principle concerning informational separation (also of power?) between the data processed by public bodies and those processed by private entities. In the EU context, one important means to ensure the availability of more personal data for law enforcement purposes is setting legally binding obligations on operators in the private sector to collect certain data, or mandating that data collected for different (usually commercial) purposes be made available for law enforcement purposes. Birnhack and Elkin-Koren underline that the State – despite the "privatization" of Internet – "never left the scene" and in the 2000s we witness a comeback of the State and a convergence of interests between private entities ( such as banks, copyright owners, service providers) and the State, leading to increased mutual informational exchanges. The invisible hand (of the online market) turned out to be very useful for the State, and it is now being replaced with the – often also invisible – handshake (Birnhack and Elkin Koren, 2008).

Much of the surveillance activity, especially in the communications or banking sector, will be conducted and analyzed by private parties (Dempsey and Flint 2004), enabling the so-called "ubiquitous dataveillance". Systematic telecommunications data retention is a paradigm for recently enhanced policies, which aim to enable and promote increased data-sharing between the public and the private domain. The case of mandatory and generalised data retention by telecommunications providers for purposes concerning law enforcement and security indicates moreover a change of legal model: communication data retention reflects a transformation from the traditional constitutional model, where evidence of wrongdoing was collected on specified suspects, to a model of intelligence-gathering, where information is gathered at random on all individuals (Levi and Wall 2004; Denninger 2002). In this latter model everyone is perceived as "a potential source of risks" or "as exchangeable element(s) in a principally dangerous environment" (Lepsius 2004).

Security is privileged over values such as freedom/liberty and autonomy in various strands of political philosophy, with an important, "traditional" role of the state being the protection of the physical security of people and property. The "social contract" was the means by which people voluntarily surrendered a certain measure of their individual freedom in exchange for the security and protection provided by a legitimate political authority. Chandler points out to risk of security theatre", i.e. the adoption of security measures of no substantial effect in order to provide the reassuring appearance of a response to perceived risks. However, "security theatre is not necessarily useless or irrational when the harmful consequences of public fear are taken into account" (Chandler, 2009). We can-

not deny that there is often strong public opinion that supports the invasion of privacy in order to achieve other policy objectives, such as public security or even consumer benefits (Surveillance Report, 2006).

## A controlling, cost-saving e-State

Moreover, under the pressure–and sometimes the pretence-of economically critical situations, State agencies concentrate their efforts on developing and implementing cost-saving policies. This is especially the case in the fields of healthcare, of social state services as well as in the taxation field. Governments are tempted to use all available information to secure cost savings and payment. The result is a growing interest in collecting, analysing and processing personal data both for controlling and planning functions. The goals are both understandable and legitimate. Institutions' needs for information on the people they deal with are infinite. However, is is not at all -and not in any case - obvious that the data in question are indispensable, adequate or "necessary" ( to use the terms of the Data Protection Directive), that leaving "needs" unsatisfied would jeopardize the efficiency of taxation authorities by identifying fraudulent returns or of law enforcement agencies by tracking suspects and suspicious behaviours.

Another important trend is the increasing number of "e"-applications such e-government, e-health, e-social security and e-justice**.** These applications are strictly related with, or actually based on data collection, sharing, matching, mining of vast amounts of personal data. Undoubtedly, such information systems and applications are not designed with an evil intent to "spy on us" but to serve us (Buttarelli, 2010a). However, these systems not only collect and record details of personal information but moreover they are organized to provide bases for action toward the people concerned **(**Rule, 2007). Such databases and applications are not without harm or security risks. Personal data, often very sensitive, which people shared with specific entities with specific purposes in mind are or will be made available to an indefinite number of recipients, or, potentially, lost or stolen, if adequate safeguards are not in place. The recent examples in UK, where data of millions of UK citizens got lost due to failure of organisational security measures, indicate the seriousness of data security risks. However, the main source of risks for informational privacy rights lies perhaps not in processing by Leviathan, the State, but in private surveillance and sousveillance, in pervasive processing by uncountable little brothers or "friends".

## Private Surveillance and Souveillance

In the expanding and borderless information market, individuals are both users and content-providers. They develop inevitably into an inexhaustible source

of personalised information. Individuals' browsing behaviour can be tracked by advertising networks across thousands of web sites. It is worth mentioning the exponential growth of the so-called "behavioural advertising", a method of tracking the online behaviour of internet users and offering of targeted internet advertising, which raises many privacy concerns [(Hotaling (2008), Buttarelli, 2010a)]. Service providers, such as search engines store all information provided by a user, such as search terms, IP addresses or browsers, and only under the strong pressure of the Article 29 Working Party, formed by representatives of Data Protection Authorities of EU Member States, search engines companies, such as Google, decided to limit the time for which this information was stored (Kosta et al., 2009). Many online business models are dependent on advertising revenue and apparently there will be continued pressure to target adverts more effectively using information on users' interests.

On the other hand, many people seem to be unaware of surveillance and of the threats it poses to their rights such as privacy and other values and interests such as dignity. Individuals are increasingly viewed as the sum of a variety of data that can be arbitrarily aggregated or taken apart and profitably marketed. Many individuals try to profit "from what is left of their privacy" (Prins, 2006). Individuals tend to think more as consumers and focus on the consumption-related opportunities and benefits that they think are "on offer" (Surveillance Report, 2006). The argumentation of free information market advocates relies on the choice of the individuals for bargaining and trading their informational privacy for services and offers (Mitrou, 2009). It is completely understandable that proponents of next generation electronic ID cards point to the fact that consumers have never rejected super-market loyalty cards and therefore have no problem with such invasive systems (EC – Privacy Challenges Report, 2010).

The tendency to exchange privacy with services or relations is reflected in a demonstrative way in social networks. Many researchers have underlined the so called "privacy paradox" (Chandler, 2009): individuals are using social networking sites to share – often without any inhibition - information not only about themselves but also about their family, friends and colleagues. A survey of Facebook users, for example, found a strong discrepancy between subjects' stated privacy attitudes and their actual privacy-protecting behaviours (Chandler, 2009). SNSs and Facebook are grounded mainly on "self-exposure", on the – cautious or incautious – decision of users to reveal information, sometimes even strict personal and sensitive, about their life. The perception of privacy, the level and quality of privacy expectations of a Facebook user are highly formulated by "trust", a key concept in SNSs and also by the architecture of online communication. Behavioral economics scholars have demonstrated that individuals' general inertia toward default terms, specified by the vendor, is a strong and pervasive limita-

tion on free choice (Korobkin 1998). Default settings as well as privacy settings are used, in order to guide or manipulate users' perceptions of their control over their profile configuration (Piskopani and Mitrou, 2009).

## Technological challenges in a world without frontiers

Global Social Networks, at the same time a replica of small communities and the Global Village, reflect also the exponential increase of online data flows. Since the adoption of the Directive we have experienced dramatic technological changes. Computer processing power has continued to follow Moore's Law, with transistor density doubling every 18-24 months – around one thousand-fold in the last two decades. Computer storage capacity and communications bandwidth have both been increasing even more quickly, doubling every 12 months and hence a thousand-fold each decade (EC – Privacy Challenges Report, 2010).

This quantitative development corresponds to a qualitative one: the multiplication of data flows has radically increased the ability of organisations to collect, store and process personal data. There is virtually no limit to the amount of information that can be recorded and there is virtually no limit to the scope of analysis that can be done (Nissenbaum, 2004). Due to technological changes we witness also a "temporal shift" (Trudel, 2009): information may be stored virtually forever. The persistency of information entails that it can last longer than the circle in which it processing was legitimate. In connection with the wide availability this persistency undermines the principles of purpose limitation and proportionality or the rights of individuals, like the right to oblivion, i.e. the right to forget and to be forgotten (Mayer-Schönberger, 2007).

Moreover, the changes in ICTs are also characterized by a "spatial shift" (Trudel, 2009): location and distance has little or no impact on the availability and accessibility of information. The Internet makes publication routine and information can easily be published outside of legitimate context and circles. The Internet and mobile information applications allow large quantities of personal data to be trivially moved between states. Vast amounts of data referring to European citizens are collected and processed through social networks, search engines and online vendors, while the applicability and – in any case - the enforceability of European law remains a controversial issue (Kosta et al., 2009). In this context we should also consider the impact of "cloud computing services": Cloud computing is a software application and data management approach utilizing web-based applications that access and store data on servers provided by third parties (Soghoian 2009). Beyond the technical definitions, we should consider that through cloud computing services the contents of e-mails, photo albums, word documents and other applications, archives/files, information systems and applications even of governmental agencies are no longer on the hard drives of our own computers but rather "outsourced" and are somewhere in an unspecified lo-

cation in the "cloud", on a server often located on another continent (Buttarelli, 2010a). The risk to be "lost in the cloud" and the difficulty to keep control over one's personal data once they have been communicated through the network is apparently especially high.

The global dimension seems to become an inherent element of processing in the digital era. Data dissemination grows together, in a dialectic relationship, with globalisation. Data are effectively linked to the flows of goods, services, finance, to the movement of persons and workers, etc. The deployment of internet, information sharing between governments and the globalization of economic activities has caused the intensification of cross borders information exchanges. Government policies, business strategies, individuals' communicative attitudes and activities tend to globalise data collection and dissemination, and to diffuse data storage (EC – Privacy Challenges Report, 2010). International flows of personal data are an obvious reality as well as the need for such flows not to be disrupted. But this reality goes together with higher or even new risks and threats with regard to the individuals' freedoms and rights. The surveillance and privacy implications are profound.

## Legal challenges in the new environment

Can the current European regulatory framework be effective in an environment of ubiquitous computing, profiling, user generated content and social networks? Should we adapt the legal principles to the Internet of Things or the convergence of "real and digitized" worlds into a seamless space for individuals, a convergence facilitated by the ever-increasing number of bridges created by both the innovative use of existing technologies and the development of new and emerging technologies? As emphasized by the Deputy European Data Protection Supervisor, G. Buttarelli, the proliferation of these bridges tends to blur the borders between environments, which may not currently be governed by the same rules, and therefore creates legal uncertainties that may undermine trust and harm the development of the Information Society (Buttarelli, 2010b).

While legislation influences social change, legislation itself is subjected to the environment, which it seeks to regulate. Evolution of ICTs may require privacy protection rules to evolve too, simply because those technological developments threaten, in new ways, the fundamental value of personal autonomy (Rouvroy and Poullet, 2009). Indeed, experience has shown that for a number of reasons, including the need to respond to technological changes and the challenges of globalization, the current data protection regime in Europe needs to be reviewed and rethought, in order to address the above presented challenges.

There are several approaches defended by theory and involved actors. Discussions of the instruments are sometimes partisan: they reflect preferences for or against state intervention or advocacy of self-regulation or technological solutions. Considering the involved actors and interests, defining the options, designing the instruments, is not at all a dispassionate technocratic process but a political process, in which there are many conflicts and interests, in which more than informational privacy is to be won or lost ( Rule, 2007).

The rhetoric seems prima facie to be in favour of the reinforcement of informational privacy. The so-called Stockholm Programme, a new multi-annual "plan" adopted in December 2009, outlines many of the measures planned for the next five years in the area of justice and home affairs, proposing a variety of measures with an enormous potential impact on privacy and fundamental rights. The Programme emphasises the commitment to respect fundamental rights and calls for a strong data protection regime as a prerequisite of the strategy.

Particular attention must be paid to the incoming European Digital Agenda, a key building block for the realisation of the EU 2020 vision, which aims to foster the development of ICT and the Internet (Buttarelli, 2010a). According to the Agenda, "The right to privacy and to the protection of personal data are fundamental rights in the EU which must be – also online - effectively enforced using the widest range of means: from the wide application of the principle of "Privacy by Design" in the relevant ICT technologies, to dissuasive sanctions wherever necessary".

## New challenges - "old" principles and new tools?

The EU has a vigorous data protection framework, which offers policy-makers, data protection authorities and courts the tools to protect 1informational privacy. The emphasis in Europe seems not to be on reinventing the principles. "The main principles of data protection are still valid despite the new technologies and globalisation" (DPWP, 2009). Principles like necessity, proportionality, data minimisation, purpose limitation and transparency have been around for 25 or 30 years and have been confirmed over and over again. They have proved their usefulness and adequacy. The emphasis should be put instead on ensuring that these "old" principles are applied more effectively in a changing ICT environment.

Moreover, the basic data protection principles and rules have, effectively, constitutional status. In any revision of the EC Directive(s) on data protection, this should be kept fully in mind. It is therefore imperative that any revised EU data protection regime (especially if it were to apply in all the areas currently covered by all three "pillars") meets the requirements of the ECHR, of the Charter and of the constitutions of the Member States. Article 51 of the Charter of the European Union states that "any limitation on the exercise of the rights and freedoms rec-

ognised by this Charter must be provided for by law and must respect the essence of those rights and freedoms". This means that limitations are only admissible for specific purposes; that they should never encroach on the essence of the fundamental rights. Such limitations must in any case also pass the so called democracy test: even if a restriction of informational privacy is foreseen by law and serves a public interest, included in the categories provided in article 8 § 2 ECHR, this restriction must still be 'necessary in a democratic society' and shouldn't reach further than what is strictly necessary. "Necessary ... is not synonymous with indispensable, neither has it the flexibility of such expressions as admissible, ordinary, useful, reasonable or desirable, but that it implies a pressing social need (ECHR, *Handyside v. United Kingdom,* judgement of 7 December 1976, § 48).

Rethinking the framework is also an opportunity to clarify the application of some key concepts such as the concept of "consent". "Consent" is an important ground for processing personal data and it is viewed as the main means to empower the data subject by exercising her right to informational self-determination. However, at the moment, it is often falsely claimed to be the applicable ground for legitimate processing, since the conditions for free given and informed consent are not fully met or the consent may end to an "consent fallacy" (Schwartz, 2000), when the (in)ability of individuals to form and express free, conscious and informed choices is reasonably questioned. This is particularly so in cases, where there is an imbalance of power: for example, in the employment context or when personal data is to be provided to public authorities. Therefore a new framework should specify the requirements for "consent" (Buttarelli, 2010a) and the cases where consent cannot serve as an adequate legal basis for processing.

A related issue concerns the users of social networks. Beyond the applicability of European data protection law in the field of social networks (Kosta et. Al, 2010), the major issues to discuss are firstly, the changing personal and social attitudes concerning exposure, privacy, disclosure and the use of information and secondly the fact that through this information use and sharing every user may become a data controller, who has to comply with procedural and substantial obligations imposed by the data protection legislation .

Legal instruments are essential, but they are not self implementing and – apparently - they are insufficient. The enforcement of data protection principles and rules remains a critical point. The role of independent supervisory authorities, such as Data Protection Commissioners/Commissions is decisive. And this is why they are mentioned in the Art. 8 of the Charter of Fundamental Rights as a specific element and requirement of the right to data protection. But their powers vary, as do their activities and their willingness or ability to act vigorously to safeguard individual and social freedoms. The powerful statutory panoply possessed by in-

dependent Authorities does not in itself guarantee the effectiveness of compliance control and, in a final analysis, of protection. It may, instead, prove to be its "Achilles' heel". The effectiveness of control is cancelled if an Authority arrives at a rationale of standard procedures and its control operation becomes entrapped in a function of providing permits, as if it were a kind of motor vehicle inspection issuing "certificates of protection of personal data" (Mitrou, 1993).

Furthermore, fifteen years after the adoption of the Directive even the way independence is guaranteed (or not) is not self-evident. In March 2010, the EU Court of Justice decided that independence means complete independence and in a case brought by the Commission against Germany, it basically said that Germany, a country with over 30 years "tradition" in the data protection field, needs to redesign its architecture and rules for supervision, in order to comply with the imperatives of the Data Protection Directive.

In discussions about the future of privacy in Europe, there are also several new tools, concepts and principles that have been less formally embedded in privacy legislation but are now presenting as central objectives and tools. Such critical principles is "privacy by design" as well as the principle of accountability.

As emphasized in the Digital Agenda 2010, the future of privacy cannot be assured solely by ex-post compliance with regulatory frameworks and "ticking off" compliance boxes. Privacy must be "designed" into ICT systems and organisational practices from the outset. Privacy by Design is actually not a brand-new concept. It was developed back already in the 1990s, meaning that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal. Devices, software, information systems, applications, services, organisational structures and practices should be designed in a privacy-friendly way, or, moreover, in a way that individuals are more empowered and exercising their rights is facilitated. It does not mean that the legal safeguards will or should be replaced by technical safeguards. It means that that they will work together. Additionally to the introduction of Privacy by Design principle, it should be also envisaged to introduce "privacy by default", in order to deal with privacy risks in fields such as social networks sites and applications.

Another key principle that is to be considered -and probably introduced into a revised data protection framework- is the principle of "accountability". In accordance to this principle, data controllers would be required to carry out the necessary measures to ensure that substantive principles and obligations laid down in legal framework are observed when processing personal data (DPWP, 2009). The data controller should, moreover, be able to demonstrate compliance, through reactive measures such as regular privacy audits and proactive measures such as

privacy impact assessments. The introduction of an accountability principle is expected to oblige organisations to build privacy in their systems and solutions so that it will form an integral "part of an organisational culture and sound governance structure" (Hustinx, 2010c). The need to provide evidence of adequate measures taken to ensure compliance will greatly facilitate the enforcement of privacy protection rules, mainly by allowing data protection authorities to use different kinds of assurance services provided by third parties and be more selective and strategic (Hustinx, 2010b).

## Global standards for global information flows?

The basic European principles should be re-affirmed and, if anything, strengthened. The present European framework is already based on the principle that whenever the responsible controller is established in Europe or equipment established in Europe is used, the installation of cookies included, for data processing the European standards will apply all over the world, regardless where the data is (Kosta et al, 2009). The issue is not at all a theoretical one: it is one of the main dispute reasons between the EU and Google, Facebook etc.

Regarding transborder data flows to third countries the European legal framework is based on the adequacy concept. The rationale behind is the desire to maintain a high level of data protection throughout the EU by preventing circumvention of EU rules through the transfer of processing o third countries with a lower standard of data protection. This solution has been firmly criticised, as it is cumbersome and slow. Reaching an adequacy determination is a lengthy process that is complicated by political factors. Kuner (in Belgium) points out that there are only 78 potential adequacy candidate countries and that it would take 130 years for these countries to be considered adequate (Kuner, 2009).

As long as global standards do not exist, diversity und (legal) uncertainty will remain Since we live in an increasingly globalised world with data being shared worldwide, it is clear that we should respond to global challenges with global solutions. Global standards would facilitate transborder data flows which, due to globalisation, are becoming the rule rather than the exception. This so-called Madrid Resolution', a Joint Proposal on International Standards adopted by the International Conference of Data Protection and Privacy Commissioners on 6 November 2009 considers international standards as indispensable. Of course there are concerns also for this approach: global standards on which level? While e.g., in Europe we have the luxury to evaluate our experiences with data protection, pondering on their reduction to merely symbolic legislation, there are other countries which, over decades now, have strived but not yet achieved to enact data protection laws at all. The Joint Proposal contains a draft of a global stand-

ard and brings together all the approaches possible in the protection of personal data and privacy, integrating legislation from five continents. It includes a series of principles, rights and obligations that should be the basis for data protection in any legal system all over the world, and demonstrates that global standards providing an adequate level of data protection are feasible in due course.[Art29-WP168]. As the European Data Protection Commissioner emphasizes this could be a mix of answers, it could be partly investing in truly global standards, it could be clarifying European jurisdiction, it could also be in facilitating international data flows (Hustinx, 2010b).

## Privacy as "necessary utopia"

Due to developments in ICTs and socio-politics personal data processing, surveillance and consequently the risks for our informational privacy have radically increased in the past decade. Despite this or exactly just because of this reality privacy remains a "necessary utopia". Informational privacy regimes offer safeguards to preserve an underlying capacity for autonomous decision - and choice-making (Mitrou, 2009). In such a perspective, the importance of protecting the individual aptitude to self-determination is not only grounded on the interests of the concerned individuals but also on the collective or societal interest in preserving a free and democratic society. Informational privacy is a precondition to exercising many other fundamental rights, such as freedom of expression, freedom of association, the right to move without being under surveillance and to be free from discrimination, rights that – exactly as privacy – are essential to democratic government because it encourages and fosters the autonomy of the individuals-citizens and creates spaces for democratic deliberation. Recently and through the introduction of invasive surveillance and processing measures, we are confronted with a "democracy paradox", i.e. the paradox that security measures intended to protect a liberal democracy can end up eroding the civil liberties at the heart of democracy. In the light of its democratic traditions, Europe should not continue giving in to surveillance temptations and "remain a model for legislation and enforcement of safeguards to privacy and freedom" (Buttarelli, 2010a).

## References

Birnjack M. and Elkin-Koren N. (2008), The Invisible Handshake: The Reemergence of the State in the Digital Environment, Tel Aviv University Law School-Tel Aviv University Law Faculty Papers Year 2008, Paper 54

Burkert, H. (2009), Towards a New Generation of Data Protection Legislation, in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), Reinventing Data Protection, Springer Science+Business Media B.V. 2009, pp 335 ff.

Buttarelli, G., Assistant European Data Protection Supervisor, (2010a), The Surveillance Policy in Europe, today and tomorrow, speech - Conference for the 30th Anniversary of the Research Center of IT and law, Namur 2010

Buttarelli, G., Assistant European Data Protection Supervisor, (2010 b), "Internet of things: ubiquitous monitoring in space and time", European Privacy and Data Protection Commissioners' Conference Prague 2010

Chandler, J. (2009), privacy versus national security - Clarifying the Trade-off in Kerr I, Steeves V. and Lucock C (eds.), Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society, Oxford University Press 2009, pp. 121ff.

De Hert P. & S. Gutwirth (2006), 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E. Claes, A. Duff & S. Gutwirth (eds.), Privacy and the criminal law, Antwerp/Oxford, Intersentia, 2006, pp. 61 ff.

Demsey, J. X. and Flint, L.M. 2004. Commercial Data and National Security. George Washington Law Review (72) 2004, pp. 1459 ff.

Denninger, E. (2002), Freiheit durch Sicherheit? Wie viel Schutz der inneren Sicherheit verlangt und verträgt das deutsche Grundgesetz?, Kritische Justiz, 35, 2002, pp. 467 ff..

DPWP Data Protection Working Party- Working Party on Police and Justice (2009), 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, Brussels 2009

European Commission – DG Justice, Freedom and Security (2010), Comparative study on different approaches to privacy challenges – Final Report, 2010.

Hildebrandt, M. (2006), Privacy and Identity, in Claes E., Duff A. and Gutwirth S (eds.), Privacy and the Criminal Law, Antwerpen – Oxford 2006, pp. 43 ff.

Hofmann-Riem, W. (2002), Freiheit und Sicherheit im Angesicht terroristischer Anschläge, Zeitschrift für Rechtspolitik, 35 (2002), pp. 497 ff.

Hotaling, A., (2008). Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting. Commlaw Conspectus. Vol. 16. (2007-2008), pp. 529 ff.

Hustinx, P. -European Data Protection Supervisor, (2010a RISE), A Privacy Framework for the Stockholm Programme, Ethical and Policy Implications of Global Mobility and Security, RISE - High Level Workshop, Brussels, March 2010

Hustinx, P. -European Data Protection Supervisor (2010b), Challenges and opportunities: the stakes are rising!, Conference Trust in the Information Society, Spanish EU Presidency, León, Spain, February 2010

Hustinx, P. -European Data Protection Supervisor (2010c), Making data protection more effective: challenges and opportunities, British Chamber of Commerce in Belgium ICT Committee - Roundtable: Data Loss Prevention – Is sensitive information leaving your organisation?, Brussels, March 2010

IPTS -Institute For Prospective Technological Studies (2003), Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview: Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs, European Communities, 2003.

Korobkin, R., (1998). Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms. Vanderbilt Law Review. Vol. 51 (1998), pp. 1583 ff.

Kosta E., Kalloniatis Ch., Mitrou L. and Kavakli E. (2009), Search engines: gateway to a new "Panopticon"?, Trust, Privacy and Security in Digital Business, Lecture Notes in Computer Science, Springer Berlin Heidelberg 2009, pp. 11 ff.

Kosta E., Kalloniatis Ch, Mitrou L. and Gritzalis S. (2010), Data Protection Issues pertaining to social networking under EU law, Transforming Government, Vol. 4 (2), 2010, pp. 193 ff.

Kuner, C. (2009), Developing an Adequate Legal Framework for International Data Transfers, in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), Reinventing Data Protection, Springer Science+Business Media B.V. 2009, pp. 263 ff.

Lepsius, O. (2004), Liberty, security and terrorism: The legal position in Germany,Part 2, German Law Journal, 5, 435, 2004

Levi, M. and Wall, D.S. (2004), Technologies, security and privacy in the Post-9-/11European Information Society, Journal of Law and Society, 31, 194, 2004.

Mayer-Schönberger V.(2007), Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing, Harvard University Faculty Research Working Papers Series, 2007

Mitrou L. (1993), Die Entwicklung der institutionellen Kontrolle des Datenschutzes - Kontrollmodelle und Kontrollinstanzen in der Bundesrepublik und Frankreich, Nomos Verlagsgesellschaft - Reihe: Frankfurter Studien zum Datenschutz, Baden-Baden, 1993

Mitrou, L. (2008), Data Retention: a Pandora Box for Rights and Liberties?, in Acquisti A., De Capitani di Vimercati S., Gritzalis, Lambrinoudakis C. (eds.), Digital Privacy: Theory, Technologies and Practices, Auerbach Publications, 2008, pp. 410 ff.

Mitrou, L. (2009) The Commodification of the Individual in the Internet Era: Informational Self-determination or "Self-alienation"? in Proceedings of 8th International Conference of Computer Ethics Philosophical Enquiry (CEPE 2009), INSEIT, Athens 2009, pp. 466 ff.

Nissenbaum, H. (2004), Privacy as Contextual Integrity, Washington Law Review Vol. 79 (2004), pp. 119 ff.

Piskopani A.-M. and Mitrou L. (2009), Facebook: Reconstructing Communication and decostructing privacy law?, in Polymenakou/Pouloudi/Pramatari (eds.), 4th Mediterranean Conference on Information Systems, Athens Greece, September 2009, CD-ROM ISBN 978-960-98566-7-6.

Prins, C., (2006), When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter? SCRIPT-ed. Vol. 3 (4) 2006, pp. 270 ff.

Rodota, S. (2009), Data Protection as a Fundamental Right, in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), Reinventing Data Protection, Springer Science+Business Media B.V. 2009, pp. 77 ff.

Rouvroy, A. and Poullet. Y.(2009), The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, in, pp. 45 ff.

Rule, J. (2007), Privacy in Peril, Oxford University Press, 2007

Schwartz, P.M., (2000). Privacy, Participation and Cyberspace – An American Perspective. D. Simon/P. Weiss (Hrsg.). Zur Autonomie des Individuums – Liber Amicorum Spiros Simitis. Nomos Verlag, Baden-Baden, pp. 337 ff.

Soghoian, C. (2009). Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era, Research Publication No. 2009-07, Berkman Center for Internet & Society, Harvard University. http://papers.ssrn.com/abstract_id=1421553. Accessed on June 1, 2010

Surveillance Studies Network (2006), A report on the Surveillance Society for the UK Information Commissioner, September 2006

Taipale, K.A. (2004), Technology, security and privacy: The fear of Frankenstein, the mythology of privacy and the lessons of King Ludd, Yale Journal of Law and Technology, 7, 2004–2005, pp. 123 ff

Trudel, P. (2009), Privacy Protection on the Internet: Risk Management and Networked Normativity, in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), Reinventing Data Protection, Springer Science+Business Media B.V. 2009, pp. 317 ff.

# Personal financial data: Regulatory framework of their e-processing focusing on the function of interbanking information systems in Greece and France

**Maria Milossi &**
**Evgenia Alexandropoulou–Egyptiadou**

## Introduction

This study aims to present the Greek and French legal framework in force on electronic processing and the legal protection of one of the most significant categories of personal data, personal financial data. The European Directives and national laws as well as the decisions of Data Protection Authorities in Greece and France (www.dpa.gr and www.cnil.fr) will be analysed.

## Personal financial data: their meaning and their content

With the term "personal financial data" or "personal data of individual economic behaviour", we mean data which refer to the individual's economic situation. They concerns an individual's property, bank accounts, financial transactions, etc.

The personal financial data run through an important part of the individual's day living, as far as almost all the parts of his social life are related to personal financial information. A person visits shops or uses the benefits of information technology (by paying with his credit card, or by logging in a website with his ID and password). This means that he may without moving from his house or his workplace, pay with electronic money, buy and sell goods and services via internet and to participate in auction sites (e-commerce), use web banking services (e-banking), make a flight reservation and pay his e-ticket (e-transport), buy a concert ticket by choosing his seat (e-entertainment), and submit digitally his tax statement (e-government).

The importance of studying the legal aspect of the individual's personal financial data lies to the fact that these are often a necessary tool for those who deal or aim to deal with this person, in order to be informed about his credit status and thus estimate the relative insolvency risks. All enterprises and mostly the banks, categorize their clients according to their transactions and their consuming habits. That is because "la valeur du client est l'intérêt du client aux yeux de l'entreprise"[1]. Thus, by creating their client's economic profile, enterprises can plan their commercial actions.

## Privacy and e-processing of personal financial data

The electronic processing of personal financial data hides many dangers for the privacy of their subject.

For instance, apart from the benefits that a web transaction offers to the data subject (that is mainly the considerable saving of money and time), the above transaction endangers the privacy of the individual concerned. This happens because every single click on the web leaves its traces on the cyber space. When a transaction takes place on the web, the company that accepts the individual's personal data has the chance to create his personal economic profile and formulate its opinion about his economic situation, his tax status as well as his consuming habits[2]. These traces on the web language are called 'cookies', that is a text string stored by a user's web browser, consisting of one or more name-value pairs, containing bits of information, which may be encrypted for information privacy and data security purposes. The cookie is sent as an HTTP header by a web server to a web browser and then sent back unchanged by the browser each time it accesses that server. A cookie can be used for authentication, session tracking (state maintenance), storing site preferences, shopping card contents, the identifier for a server-based session, or anything else that can be accomplished through storing textual data. Cookies' usage enables the fast information flow and reduces the time needed for the user to reenter to the same web page[3]. However, this procedure enables the suppliers to organize the web visitors' data, in order to treat them and then exploit them for commercial purposes, some times without the consent of the interested person.

For the accomplishment of the said purposes, different mathematical methods[4] are being used from the companies such as: a. Credit scoring: It is one of the most successful applications of statistical and operations research modeling in finance and banking. It is the set of decision models and their underlying techniques that aid lenders in the granting of consumer credit. These techniques decide who will get credit, how much credit they should get and what operation strategies will enhance the profitability of the borrowers to the lenders. b. Data Warehouse: A data warehouse is a repository of an organization's electronically stored data. Data warehouses are designed to facilitate reporting and analysis. The means to retrieve and analyze data, to extract, transform and load data and to manage the data dictionary are also considered essential components of a data warehousing system and c. Data mining**:** It refers to the process of extracting patterns from data. Data mining is becoming an increasingly important tool to transform this data into information. It is commonly used in a wide range of profiling practices, such as marketing, surveillance, fraud detection and scientific discovery.

One of the results of all these methods is the spamming, that is defined as the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media (junk fax transmissions, social networking spam, television advertising and file sharing network spam, etc). Spamming is universally criticized and has been the subject of legislation in many jurisdictions. Greece and France have implemented under this Directive, 2002/58/EC Directive on privacy and electronic communications the consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, shall have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including ticking a box when visiting an Internet website.

## Fields of e-processing of personal financial data

E-commerce is the most common example of "place" where we link personal data with economic behaviour. E-commerce consists of buying and selling products or services over electronic systems as well as the exchange of data to facilitate the financing and payment aspects of the business transactions. The main advantage of e-commerce is that the sale and purchase transaction is completed electronically and interactively in real-time. For the transaction's accomplishment, appropriate software is necessary to permit the electronic data interchange (EDI) between the parties that participate to the transaction[5]. This interchange is the structured transmission of data between organizations by electronic means. It is used to transfer electronic documents from one computer system to another[6], as for example from one trading partner to another.

The most characteristic forms of e-commerce are web banking, electronic auctions as well as distance marketing of financial services. A general framework to cover certain legal aspects of electronic commerce in the internal market was provided the Directive 2000/31/EC[7] which has been implemented to Greek law by the presidential decree 131/2003 and in French law by the law 2004-575. The use of computers and telecommunications to enable banking transactions by telephone or computer rather than through human interaction is called electronic banking[8]. Electronic banking has vastly reduced the physical transfer of paper money and coinage from one place to another or even from one person to another.

Besides, electronic auctions have emerged as a major part for e-commerce, especially in Europe. Electronic auctions are realised with the participation of consumers and of business (business to consumer) or between the business (business

to business, B2B). For the inscription on an auction site, a credit card number, a phone number and the address of the customer are necessary. Moreover, in Belgium an electronic identity card is needed to enter an auction site[9]. In Greece, no special legislation on electronic auctions exists. However, the legal framework that regulates electronic auctions is Directive 2000/31/EC (especially the articles 18 et seq), as well as the presidential decree 131/2003 which implemented the directive in the internal law. In any case, for this type of e-commerce the provisions for distant contracts are followed[10]. In France, electronic auctions are regulated by the law 2000-642 that implemented the Directive.

The fundamental text about distance marketing of financial services is the European Union's Directive 2002/65/EC which regulates the sale of pensions, mortgages and other financial services and products by means of distance communication. Distant communication includes sales taking place on-line or by e-mail, telephone, fax or regular mail. In this Directive, significant terms are defined such as: distance contract, distance communication, financial service, supplier, consumer, and means of distance communication. The Directive's main goal, is to encourage competition between suppliers throughout Europe and its' Member States. Many financial services, such as banking, credit, insurance, personal pensions, investment or payment services, are being sold at a distance, with consequent cost and access benefits for consumers and sellers alike. The Directive also aims to ensure that consumers using distance sales channels are not at a disadvantage to those using the traditional sales channels. The consumer should have confidence in the security of the transaction, which in turn should lead to increased use of new technology for the sale and purchase of financial services. In Greece the Directive was implemented into national law by the law 3587/2007 and in France by the decree 2005-1450.

Another field where e-processing of personal financial data takes place is e-government. E-government is the use of Information & Communication Technologies (ICTs) to render public administrations more efficient and effective to the people who need to use them (ec.europa.eu/information_society/activities/egovernment). ICTs are already widely used by government bodies, just as in enterprises, but e-government involves much more than just the tools. E-government enables all citizens, enterprises and organisations to carry out their business with government more easily, more quickly and at lower cost.

In the European Union's internal market, people are able to move freely-either for work or for other reasons-and consequently they have to be able to deal with public services in different countries. Then it is crucial that different government bodies, both within a country and in different EU Member States, are able to share information easily and co-operate in serving citizens.

E-government, enables individuals to proceed in transactions with public services, in order that they arrange fast and safely all these matters that concern their economic, tax, professional or property situation.The Lisbon Strategy on 2000 as well as the Treaty of Lisbon, were the main texts that regulated e-government.

In Greece, example of e-government is the online tax declaration to the general secretariat for information systems of the Ministry of Economic and finance (www.gsis.gr), the online submission of ownership declaration to the Hellenic (www.ktimatologio.gr), as well as the online application for the pension and insurance matters via the site of Citizen's Service Centers (KEP, www.kep.gov.gr). Similarly in France, where the term "electronic administration" (administration électronique) is preferred to instead of e-government, the citizen has the ability to submit online his tax declaration (www.impots.gouv.fr) and be informed for it in real time, to pay online fines issued by automated traffic enforcement cameras (radars) and all fines where the payment counterfoil contains an e-payment reference (www.amendes.gouv.fr), as well as to make an online application for the granting of family allocation of social security (www.caf.fr).

## The regulatory framework of personal financial data's e-processing in the banking sector in Greece and France

Despite the fact that until 1995 almost all the Member States of the European Union, enacted laws about the protection of individual's privacy, the first fundamental legal text regulating the processing and the legal protection of personal data (including personal financial data) was the Directive 95/46/EC on "the protection of individuals with regard to the processing of personal data and on the free movement of such data.

This Directive (known as the European Data Protection Directive) gave Member States the guidelines for the implementation into their national law. Thus, in compliance with the Directive (art. 2), personal data means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to, should be taken into consideration. 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 processing of personal data is any operation or set of operations in relation to such data, whatever the mechanism used, es-

pecially obtaining, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction. A personal data filing system means any structured and stable set of personal data that are accessible according to specific criteria. The data subject of a processing of personal data means an individual to whom the data covered by the processing relate.

Greece implemented the Directive with the law 2472/1997[11] and France implemented it by law 2004-801 (which amended the law n°78-17 of 6 January 1978 on data processing, data files and individual liberties[12)]. According to the Directive's provisions (see article 8 case 1 of 95/46/EC) financial data are considered to belong to the category of the simple data and not to sensitive ones, despite the fact that they refer to a strictly private field of an individual's life. The reason that justifies this differentiation is the need for transparency and for fight of money laundering, a need which probably couldn't be satisfied if a special status of protection would have been recognized to this category of personal data[13].

In Greece, according to the amendment of article 2 case b of law 2472/1997 by the article 18 par.1 of law 3471/2006, the list of "sensitive" called personal data has been restricted. While in the former legal framework participation in any kind of association was considered to be sensitive data, after the law's amendment, only the participation in a trade union or in an another association related to sensitive data is considered as sensitive data[14], for example participation in an association of adopted children or persons with a disability.

In case of infringement of the provisions of this legal framework, administrative, civil and penal sanctions follow.

In order to better understand the regulatory framework of personal financial data's electronic processing in the banking sector in Greece and France, we have to examine the function of interbanking information systems, the principles according to which the data are being processed, the data's recipients as well as the related rights of the individual concerned.

## *Interbanking information system in Greece*

In Greece, an interbanking company named TIRESIAS (www.tiresias.gr) processes data that reflect the economic behaviour of individuals and companies as well as data that contribute to the prevention of fraud in financial transactions. Members of the TIRESIAS system are all the Greek Banks which entrusted it with the development and the management of a reliable Credit Profile Databank. The data stored in the TIRESIAS system contribute to the protection of credit, the reduction of credit risk and the improvement of financial transactions, to the benefit of

individuals and the banking system in general. The correct estimation of solvency and the financial credibility of banks' clients contribute to the decrease of bad debts resulting to the decrease of cost of loans and of the citizens' debts.

TIRESIAS operates on the principle of respect and protection of public the law 2472/97 on the "Protection of the individual from the processing of personal data" and the relevant provisions of the Directive 95/46/EC. Due to the fact that the credit profile data of individuals is of personal nature, their processing is subject to the provisions of Law 2472/97[15]. However, this data's category doesn't belong the "sensitive data" category, as defined in the above law. The TIRESIAS system has developed and operation of the Credit Profile Database and the Risk Consolidation System, in order to assure the individual's protection from the illegal processing of such data. The TIRESIAS system organised personal financial data in four files called "systems": 1. The Default Financial Obligation System (DFO) & Mortgages and Prenotations to Mortgages System (MPS), 2. The Credit Consolidation System, 3.The lost or stolen Identity Card and Passport System (IPS) and 4. The Terminated Merchants System (TMS).

## The Default Financial Obligation System (DFO) & Mortgages and Prenotations to Mortgages System (MPS)

This system contains data (e.g. bounced checks, liquidation auction announcements, bankruptcies) on the credit behaviour of individuals and companies. Both DFO & MPS aim at supporting a more accurate assessment of the financial credibility of the clients (current or future) by the banks. The Mortgages Prenotation to Mortgages System contains the respective data for mortgages and prenotations.

## The Credit Consolidation System (CCS)

This system contains data concerning consumer and housing loans, credit cards of natural persons and credit to small and medium-size businesses (with annual revenue less than 2,5 million Euro). It contains information about the status of the credit (current balance with no delinquency, delinquent balance etc). The function of the Databank and all the relevant activities secure the regular collection of data from credit/financial institutions regarding possible debts from loans, their processing, the completeness control as well as the dissemination of the processed information. Access to this file is possible with the consent of the interested party. In the case of consent withdrawal, an indication is noted, that is evaluated by the bank.

## The lost or stolen Identity Card and Passport System (IPS)

This system is an auxiliary Databank on declarations (submitted either directly to TIRESIAS or via the Ministry for the protection of citizens) of lost or stolen ID

cards and passports. The purpose of this database is to keep the wider banking sector in general informed in order to protect transactions and clients from potentially consequential damages resulting from loss or theft.

### The terminated Merchants System (TMS)

This system contains information about merchants whose contracts for accepting credit cards as means of payment have been terminated by the banks. The termination of these contracts takes place due to fraudulent activity. The database does not include sensitive information on card usage or their owners' personal data. This file aims to contribute to the protection of credit provided by banks and assuring reliable financial transactions. This purpose is attained through the provision to financial institutions of access to the database previously mentioned, therefore enabling them to evaluate risks undertaken while signing a contract with a specific merchant. Access to this database is provided for private use to the departments of credit institutions and payment card operators that are authorized for signing contracts concerning card acceptance with merchants.

### *Interbanking information system in France*

In France, the Bank of France (www.banque-france.fr) organized its filing systems containing personal financial data and reflecting individual's economic profile in order to evaluate the trustworthiness of banks' clients and protect them from personal debt problems. These filing systems operate and process clients' personal data according to the provisions of the law 78-17 as it was amended by the law 2004-801. To accomplish this mission, the Bank of France has provided a secretariat for the household debt commissions. The commissions, set up in each French department (that is an administrative unit), are charged with finding solutions to the problems encountered by individuals who have incurred excessive debts or who experience financial problems due to unforeseeable events. According to the law 2003-706, the commission may, depending on the gravity of the financial difficulties faced by the debtor, direct the case: i) either towards an out-of-court procedure based on the negotiation of an agreed repayment schedule liable to be accepted by the debtor and his creditors or ii) towards a personal recovery procedure - based on personal bankruptcy procedures - when the debtor's situation is "irremediably compromised". In its role as administrator of the household debt commission secretariats, the Bank of France is charged with receiving debtors' applications and processing their cases, notably by conducting, on the commission's behalf, negotiations with creditors and drawing up recommendations to be submitted to the courts.

For this purpose, the Bank of France created and operates under its control: 1.The Central Cheque Register (FCC), 2. The National Register of Irregular Cheques

(FNCI), 3.The National Database on Household Credit Repayment Incidents (FICP) and 4. The National hotline for lost or stolen cheques (CNACPV).

Moreover, CNIL has authorised several subsidiaries of banking groups, specialized in consumer credit (such as Credit Agricole in 2005 with Finaref and Sofinco; BNP Paribas in 2006 with Cetelem and Cofinoga) to share data on their borrowers for purposes of bad debt prevention, based on five criteria: a. the legitimacy of purpose: (for example the prevention of fraud and bad debts) b. the occasional and restricted nature of data exchanges between the credit institutions, (no centralized database is created). Client records kept by the institutions cannot be fused with any data transferred via the query system c. the quality of institutions granted authorization to exchange data, when all are consumer credit specialist companies, hence all bound by banking secrecy d. the existence of a shared financial risk between these institutions, reflected in an effective control by certain companies over others, or in third-party risk management and e. the explicit authorization given by the client to share data covered by the banking secrecy, requiring among other that the client be clearly informed of the purposes and recipients of the shared data.

However, CNIL has not authorized other institutions which could not fulfill the above criteria (e.g. the case of the companies Experian and Infobail).

## The Central Cheque Register (FCC)

The Central Cheque Register, created in 1955 as a result of the public authorities' and banking industry's desire to encourage the use of cheques by making them more secure. The law 91-1382 on the security of cheques and payment cards amplified the Bank of France's role in the prevention of the issuance of bad cheques. The legal provisions relating to cheques and, more specifically payment incidents have been incorporated in the French Monetary and Financial Code (Articles L. 131-1 et seq). The Bank of France keeps a central record of payment incidents involving bad cheques, bank-imposed bans on writing cheques that are systematically imposed on account holders that causes these incidents, and court-ordered bans on writing cheques.

## The National Register of Irregular Cheques (FNCI)

The national register of irregular cheques (FNCI) centralises bank details on all accounts opened by persons banned from writing cheques, stop payment orders resulting from loss or theft of cheques, account closures and the characteristics of counterfeit cheques. According to the article L.131-86 of the French Monetary and Financial Code, the Bank of France is responsible for providing information on the regularity of all cheques that it is likely to accept in payment of goods and services. The banks transmit this information to the FNCI in accordance with the provisions

of Article L. 131-84 of the Monetary and Financial Code and Articles 19 and 28 of Decree 92-456 of 22 May 1992. The FNCI also centralises reports of loss or theft of chequebooks made by victims to the National hotline for lost or stolen cheques. These reports are kept for 48 working hours after which they need to be confirmed by a stop payment order from the bank that holds the account.

According to the provisions of the Article 4 of the Decree of 24 July 1992, the Bank of France has entrusted a private company with the task of implementing FNCI consultation procedures. The service that gives access to the FNCI is called VERIFIANCE-FNCI- Bank of France. In order to consult the FNCI, the users must scan the «CMC7 strip», that is the magnetic strip that is located at the bottom of the cheque. Various colours transmit various types of information to retailers Thus, the green colour means no information in the FNCI, the white colour means that the cheque cannot be read, the red colour, means that the cheque is irregular (that is ban on writing cheques, closed account, stop payment order due to loss or theft, counterfeit cheque), the orange colour means that the bank account is under a stop-payment order due to loss or theft (with no indication of cheque numbers) or a report to the National hotline for lost or stolen cheques.

## The National Database on Household Credit Repayment Incidents (FICP)

The FICP was created on 1989, in accordance with the provisions of the Act of 31 December 1989 on Preventing and Resolving Personal Debt Problems that have already been incorporated into the Consumer Protection Code under Articles L 333.4 to L 333.6 The system is organised around household debt commissions with at least one for each department (department is the French administrative unit). These commissions work with the creditors of people facing debt problems in order to try to achieve out-of-court agreement and reschedule the debts. If all this procedure fails, the debt commissions can propose specific measures that will be binding on the parties, following approval by the who handles the case.

The FICP's primary aim is to provide credit institutions with information that will help them assess the repayment difficulties encountered by individuals. The Article L333-4 of Consumer Protection Code defines the content of the database. That is: a. the payment incidents about non-professional loans to individuals b. applications filed with the debt commissions, c. mutually-agreed or court-ordered work-out measures to deal with cases of overindebtedness, including personal bankruptcy measures (Act 2003-710 of 1 August 2003) and d. the civil bankruptcy rulings made in the Alsace and Moselle departments.

In fact, the National database on household credit repayment incidents (FICP), administered by the Bank of France, is the key tool in the prevention of over-

indebtedness. Being listed in the FICP does not prevent credit institutions from granting loans, but FICP is designed to provide them with information so that they can better assess their risks in this area of activity.

The FICP records this information for persons who stay in metropolitan France, the overseas departments and Saint Pierre and Miquelon. It also collects information on French citizens who reside outside France in respect of non-professional loans. Since the 1st of April 2007, the rules of the Regulation 90-05 (amended) of 11 April 1990 have been applicable to the overseas units of New Caledonie, French Polynesie, Wallis and Futuna and the territorial unit of Mayotte.

## The National hotline for lost or stolen cheques (CNACPV)

The National hotline for lost or stolen cheques was set up by the Bank of France in 1996. It is open seven days a week and 24 hours a day and allows cheque book holders to report the loss or theft of cheque books to the National Register of Irregular Cheques (FNCI) by telephone, as soon as the incident occurs, and, most importantly, when banks are closed. Once the report is recorded in the FNCI, an alarm is set off should the lost or stolen cheque be scanned by a retailer that subscribes to the VERIFIANCE-FNCI-Banque de France service (it is the service which permits the access to the National Register of Irregular Cheques, www.verifiance-fnci.fr), the FNCI consultation system. Reports are deleted after 48 working hours if they are not confirmed by stop-payment orders issued by the account holding bank and reported to the FNCI. Account holders must therefore transmit written stop-payment orders to their banks as soon as possible in accordance with the provisions of Article L 131-35 of the French Monetary and Financial Code.

### *Operational principles applied to the processing of personal financial data*

In order to be lawfully processed, financial data must be collected fairly and lawfully for specific, explicit and legitimate reasons in view of such purposes according (article 6 of law 2472/1997 and of law 801-2004). In our case, banks' purpose for processing personal financial data is the minimization of the risks involved while signing credit contracts with uncreditworthy clients, as well as the minimization of the creation of doubtful debts, in the protection of commercial credit as well as in the improvement of economic transactions (principle of scope). The data processing is justified as "absolutely necessary" for the achievement of the said purpose, while the protection of commercial credit compared with the interests of the data subjects, may be considered to "evidently prevail" over them, in the sense of Art. 5, par. 2, section e, according to the DPA'S decision No 109/1999 repeated by the DPA'S decision No 24/2004. Consequently, processing is allowed even without the consent[16] of the data subject, pro-

vided that the latter has been informed (Art. 11, par. 1 and Art. 24, par.3, Law 2472/1997).

Additionally, data concerning purchasing and selling of real property, must not be processed as they are found to be incompatible with the principle of proportionality, according to which data «must not be excessive in relation to the purposes for which they are processed at any given time» in compliance with the Art. 4, par.1, section b Law 2472/97[17] and article 6 par. 3 of the law 2004-801. Maintenance of such data in advance for an indefinite number of persons who do not have (and maybe never will) any contractual relation with banks far exceeds the purposes of the file (principle of proportionality). Processing of the above data is allowed only with consent of the data subject.

Besides, in order to be lawfully processed, personal data must be accurate and where necessary kept up to date. Especially in the banking field, where the individual's data are kept in specific files with long storage time, controllers must be more attentive. For example, when the name of the individual concerned is very common e.g. Papadopoulos, the controller must add further identifying elements such as mothername, date of birth, etc. However, the only responsible part to update the individual's data status is the controller (principle of accuracy) in case that the new elements, as for example payment of debt, result from a public file[18]. On the contrary, if the new elements (e.g. payment of debt) do not result of a public file, then the person concerned must inform the controllers about the change of data's status.

Moreover, personal data shall be stored in a form that allows the identification of data subjects for a period no longer than necessary for the purposes for which they are obtained and processed (principle of respect of storage time), as it will be presented in the following paragraph.

### *Storage time of personal financial data*

One of the most important aspects of the protection of personal financial data is their maintenance and their storage time in the individual's reference file by the controllers. Directive 95/46/EC as well as the text of Greek and French law about the protection of personal data, adopt the principle that a data processing may last for a period during which the controller intends to carry out data processing or maintain the file (article 6 section e of laws 2472/1997 and 2004-801).

Of course, it is another matter, if historic, statistical or scientific reasons lengthen personal data storage time, in condition that these data are not related to a particular subject. The nature of personal financial data signals it's duration in the reference file. This means for example, that according to the article 3 of the recent law 3816/2010, in the TIRESIAS system the bounced checks and unpaid bills of

exchange are stored for two years, liquidation auction announcements and confiscations and seizures are stored for four years, bankruptcies are stored for ten years and at the same time Mortgages, Prenotations of Mortgages, conversions of prenotations to mortgages' storage time expire when these are avoided.

Similarly, in the French interbanking information system, if the debt commission finds that a debtor's situation is permanently impaired, it may direct the case towards personal bankruptcy proceedings, which are recorded in the FICP for eight years (L 332-11 Consumer Protection Code). Moreover, once debtors have fully repaid creditors named in mutually-agreed or court-ordered measures, these work-outs must be deleted from the database immediately. With the exception of the partial cancellation of debts, personal recovery procedures and personal bankruptcy measures can be rescinded at any time, provided that the debtor supplies proof of full payment of the sums due from each of the creditors concerned. According to the CNIL'S recent position, the storage time has to be reduced for certain categories of data (data concerning over indebtedness), from ten to eight years [20].

The data's storage time, not only for the personal financial data but for the personal data in general, is based on the right to oblivion (or the right to forget) which protects an individual's privacy and protect him from being permanently held to ransom by unfortunate actions from his past.

### *Recipients of personal financial data*

Recipients are considered to be the persons to whom data are expected to be communicated. In Greek as well as in French information banking system, only banks, financial institutions, credit card companies and public sector entities are justified to be recipients of data, in consistence with the purpose of the processing. On the contrary, third parties in economic transactions and non-parties are not justified to be recipients of such data. It is self-evident that only the above recipients of personal data have the right to use them. Further processing, transfer to third parties etc. is completely prohibited. TIRESIAS must comply with the obligation to inform the data subject (see article 24 par. 3 in combination with the Art. 11, par. 1 of the Law 2472/1997). Especially, in Greek interbanking information system, factoring and leasing companies are also recipients (Data Protection Authority decision 523/1999). On the contrary, insurance companies which insure credits are not considered to be recipients (DPA'S No 62/2003 decision).

The data subject has to be informed during the collection stage about the recipients (art. 11 of law 2472/1997 and 11 of law 2004-801), as well as about the addition of other recipients or of another category of recipients a posteriori (after the data collection but before the transfer to the recipient). It has to be men-

tioned that there is not an obligation for TIRESIAS to inform the subject about every specific transfer made by it when asked by the recipient. This obligation belongs to the recipient (bank et.c.)

### *Individual's rights related to his personal financial data's e-processing*

As we have already seen, according to the articles 11 of Greek law 2472/1997 and 32 of French law 2004-801, the Controller must, during the stage of collection of personal data, inform the data subject in an appropriate and express manner of the following data about his identity and the identity of his representative, if any, the purpose of data processing, the recipients or the categories of recipients of such data as well as about the existence of a right to access.

If the Controller, in order to collect personal data, requests the data subject's assistance, he must inform him specifically and in writing. By means of such notification the Controller shall also inform the data subject whether he is obliged to assist in the collection of data, on the basis of which provisions, as well as of any sanctions resulting from his failure to co-operate. When the Controller processes datas of a considerable number of persons (over 1000), he may inform them about the processing of their data via press (newspapers e.t.c.) deviating from the general rule of in concreto information [21].

Apart from the right of information, the individual whose personal data are being processed or have been processed has also the right to access to his data (see the article 12 of the law 2472/1997 and the article 39 of the law 801-2004). Especially he has the right to access to all personal data relating to him as well as their source, the purposes of data processing, the recipient or the categories of recipients, any developments as to such processing for the period since he was last notified or advised, the logic involved in the automated data processing, the correction, deletion or locking of data, the notification to third parties, to whom the data have been announced, of any correction, deletion or locking, taken that the notification is not impossible or does not demand disproportionate efforts. The right of access is exercised by means of a relevant application to the Controller, who must answer in writing, without delay and in a clear and express manner. All persons may obtain information about their data's processing by going in person to customer service and information offices. Persons wishing to contest and, where appropriate, amend database information in their name, must submit a request to the reporting institution either by physical presence to the bank or by post .

Besides all the above, the individual has also the right to object (article 13 of the greek law 2472/1997 and the article 38 of the French law 801-2004) at any time to the processing of data relating to him. Such objections shall be addressed

in writing to the Controller and must contain a request for a specific action, such as correction, temporary non-use, locking, non-transfer or deletion. Moreover, any person shall be entitled to declare to the Authority that he does not wish data relating to him to be submitted to processing in order to promote the sale of goods or long distance services. The Authority shall keep a register for the identification of such persons.

## Conclusions and final thoughts

The new ethics that brought the technology's progress was the reason that changed the "legal spirit" about individual's privacy and economic behaviour. Conservative or not, the fundamental European texts as well as the Greek and the French national legal framework remind us the challenge of balancing between the maintenance of technology development and the protection of individual's private life. In this study, it is obvious that national and European legal framework (including the decisions of National Data Protection Authorities) try to get the balance right between the banks' (credit enterprises') profits and their clients' rights.

It is certain, that the regulatory framework on the e-processing of personal financial data can be developed and be more complete in case that citizens-bank clients have the sensibility to appeal to the Data Protection Authorities and banks show their interest to resolve daily problems (coming from this processing), often with the help of the above Authorities. Additionally, it would be crucial to the protection of personal financial data, to enact special and detailed guidelines coming from the Data Protection Authorities (soft law). As a result, the function of the banking system will be further defined and the security of transactions will be improved. Moreover, an important step to personal data protection could also be the enactment of a law concerning not only the natural persons but also legal ones, given that companies consist the majority of banks' customers[20].

## Endnotes

1. Girot, J.L.(2005), Le harcèlement numérique, DALLOZ, p. 60.
2. Chatillon, G. (2007), Les données personnelles: enjeux juridiques et perspectives IDT juin 1999, dimanche 13 mai 2007, online at: www.georges-chatillon.eu/accessed 14.06.2010.
3. Alexandridou, E. (2004), The e-commerce law- National and European, Sakkoulas, Athens-Thessaloniki, p. 185.
4. Iglezakis, I.(2003), The legal framework of e-commerce, Sakkoulas, Athens-Thessaloniki, p. 211.
5. Sinaniotis-Mavroudis, A.-Farsarotas, I. (2005), Electronic banking, Ant. N. Sakkoulas, Athens-Komotini, , pages 114-116.

6. Maisl, H. (1996), Le droit des données publiques, L.G.D.J,page 51.

7. Karakostas, I. (2003), Law & Internet-Legal aspects of internet, P.N. Sakkoulas, p. 165.

8. Yiannopoulos, G. (2003), Internet Banking –Legal questions about internet banking transactions, Internet Banking Legal aspects, Deltion of Hellenic Bank Association, 3 rd semester, p. 97, online at: www.hba.gr/accessed 14.06.2010.

9. Wery, E. (2008), Première mondiale: le site belge d'eBay utilise la carte d'identité électronique pour authentifier les utilisateurs, article of 28/02/2008 online at: http://www.droit-technologie.org/actuality-1123/premiere-mondiale-le-site-belge-d-ebay-utilise-la-carte-d-identite-e.html, accessed 14.06.2010.

10. Verbiest, T. (2000), Les ventes aux enchères électroniques: quel cadre juridique? online at www.droit-technologie.org/actuality-344/les-ventes-aux-encheres electroniques-quel-cadre-juridique-chroni.html/accessed 14.06.2010.

11. Alexandropoulou-Egyptiadou, E (2007), Personal Data-The legal framework of their electronic processing, A.N. Sakkoulas, Athens-Komotini, p. 29 et seq.

12. Devèze J., Lucas J. & Frayssinet J.: Droit de l'informatique et de l'Internet, THÉMIS, PUF, PARIS 2001, p. 1 et seq.

13. Iglezakis, I. (2003): Sensitive Personal Data, Sakkoulas, Athens-Thessaloniki, p. 94.

14. Alexandropoulou-Egyptiadou, E (2007), Personal Data-The legal framework of their electronic processing, A.N. Sakkoulas, Athens-Komotini, p. 36 and the references thereof.

15. Saatzidou-Panteliadou, E. (2007), New law regulations in New Economy – The electronic processing of data of economic behaviour, Giahoudis, p. 113.

16. Alexandropoulou-Egyptiadou, E (2007), Personal Data-The legal framework of their electronic processing, A.N. Sakkoulas, Athens-Komotini, p. 33-34, footnote 15.

17. Alexandropoulou-Egyptiadou, E.(2007), Personal Data-The legal framework of their electronic processing, A.N. Sakkoulas, Athens-Komotini, p. 57 et seq.

18. Alexandropoulou-Egyptiadou E (2004), The electronic processing of personal data in banking field-The legal framework, Armenopoulos, p. 1377.

19. Alexandropoulou-Egyptiadou, E (2004), The electronic processing of personal data in banking field-The legal framework, Armenopoulos, p. 1391.

20. CNIL's paper: Vers une réforme crédit à la consommation et des fichiers de crédits, 26 mai 2010, online at: www.cnil.fr/dossiers/argent/actualites/article/238/vers-une-reforme-du-credit-a-la-consommation-et-des-fichiers-de-credits/ accessed 14.06.2010.

21. Alexandropoulou-Egyptiadou E. (2004), The electronic processing of personal data in banking field-The institutional framework, Deltion of the Hellenic Bank Association, p. 30.

22. Alexandropoulou-Egyptiadou E. (2004), The electronic processing of personal data in banking field-The legal framework, Armenopoulos, p. 1395.

# You want even more personal data? Are you kidding?

**Klemen Mišič**

*Those who would give up Essential Liberty to purchase a little Temporary Safety, deserve neither Liberty nor Safety (Benjamin Franklin)*

## What is the cause and what is the consequence?

***Cause***: Christmas, 2009: Abdul Farouk Umar Abdulmutallab, Nigerian citizen, wants to detonate plastic explosives hidden in his underwear while on board of the plane en route from Amsterdam to Detroit.

***Consequence***: Airports across the world introduced the notorious *body scanners*.

Have you already seen the picture taken by a body scanner? If not, let me inform you – on the picture taken with the body scanner, you are naked. OK, you can say *it's for my safety*, but let me rephrase the question – would you mind, if the security in the front of the supermarket took you to some small cabin and told you to undress in front of them? Just to check you don't have any hidden weapons on yourself. Where is the difference?

Let's talk a little bit about the cause and the consequence. Is it really as I wrote above and as it seems to be? No. The first question we have to ask ourselves is *why did the Christmas bomber want to blow up the plane*.

Let's put the political statements of some countries aside – we cannot influence foreign politics. And, frankly, probably we also don't want to. But, what is interesting for us is that (not only) American agencies began to collect huge databases of Personal Data from passengers who travel by plane (PNR). However, huge databases also mean huge statistic work and *data mining*. Algorithms for data mining need to be set up very precisely to get the best results from data. But even if someone sets up the algorithms as accurately as one can, statistical mistakes[1] are still possible. When the data processor collects too much data (Personal Data), there is *always* a possibility of huge mistakes.

Obviously that is just what happened with Mr. Farouk Umar Abdulmutallab. Just after the attack, the news even spread around some rumours, that his father had called some of US authorities and informed them about his son's plans[2]. And even if I assume these are really *only* rumours, the airport system check failed. The real

question is why did the system fail? I'm afraid we still don't have the answer on this quoestion, but new security measures are introduced on airports worldwide *anyway*.

So, what can we learn from this case? My assumption is that the authorities didn't recognize the patterns in this case or the supercomputers weren't able to isolate Mr. Farouk Umar Abdulmutallab's Personal Data out of the huge database. The system failed. So, the real cause for putting *body scanners* on the market (I don't want to put this debate on the level of great marketing move for selling body scanners at the most appropriate time) wasn't the *Christmas bomber*, but the absence of reliable data mining and better airline security.

At this point we come to another absurd situation. Because the state authorities (not only US, but also Netherlands' authorities, where Mr. Farouk Umar Abdulmutallab's departed) failed with the security checks and data mining, the same states ignited the chain reaction of body scanners on airports worldwide. It kind of reminds me on a children's thinking, when something bad happens to them. They don't blame themselves for the mistake; they find other children and release their anger on them. And now the same situation in the world of adults: the state authorities failed to bring us security, but the price for that shifted on us, the "usual" citizens. Now we have to pay for the lack of security with our privacy. And at this point we should recall the quote of Benjamin Franklin, written above - *Those who would give up Essential Liberty to purchase a little Temporary Safety, deserve neither Liberty nor Safety*. What do we do – we let the states collect even more of our Personal Data and invade our Privacy (both Human Rights) in exchange for our "security". So, do we deserve Liberty or Security?

Any doubts in answering the latter question will be removed by next case. The German TV station ZDF broadcasted a show[3] in which one of the experts showed that body scanners aren't reliable. He was able to pass the body scanner with some strong chemicals, which can burn through the airplane casing.

So, what've bought with our Privacy and Data Protection? Actually nothing. Body scanners can detect guns and knives, but not chemicals. We all know that criminals are most of the time one step ahead of the law. So now we maybe really chased away the guns, but we got chemicals, which are no different from the guns. They can for example cause the same result as the guns or bombs on the plane – they can crash the plane.

So, what is my point of these stories? Simple: if I change a little Queen's *Too much love will kill you,* I can write: "*To much Data will kill you*". There is no use in collecting too much Personal Data, since the more Data someone has, the bigger the mistakes that can happen[4]. And the *real* consequences of the safety mistakes

can be very destructive. Or if I quote Mr. Michael Bloomberg, mayor of NY City: "*There are lots of threats to you in the world. There's the treat of a heart attack for genetic reasons. You can't sit there and worry about anything. Get a life … You have a much greater danger of being hit by lightning than being struck by a terrorist.*"

## Biometrics is modern. It's everything. Really?

**1995**: Mr. Raymond Easton gave his DNA sample to the British police during a domestic dispute.

**1999**: Mr. Easton was visited by British police and asked to give a DNA sample to help the police with an investigation of a burglary nearby. Few hours later he was in the police cell, where he was kept for several hours. The police found his DNA at the crime scene. Here's the surprise: Mr. Easton was suffering from advanced Parkinson's disease and was unable to dress himself or walk more than few meters unaided. He was arrested on the ground of burglary. But Mr. Easton with his disease obviously wasn't able to commit the crime. So, what happened? Mr. Easton was a victim of so called *cold hit*. The sample points (6 points) on his DNA matched to the criminal's DNA sample points. The possibility that this could happen is 1:37.000.000, but *it happened*. After the discovery it still took three months for the charges against him to be dropped. So, it seems appropriate to warn that biometrics – from this perspective at least – is not an almighty and error free way of identification, and should not, therefore, be blindly trusted.

According to Wikipedia[5] the US DNA database maintains over 5 million records as of 2007, the UK the same number, despite the UK has smaller population.

Slovene legislation is one of the first legislations in the world which implemented rules for biometric use in the Personal Data Protection law. Fingerprints – as with the iris, retina, facial features etc. – provide sources of biometric data which represent characteristics that are unique and attributable solely to each and every individual; as such, and as a characteristic by way of which a person is identified or at least identifiable, they undoubtedly represent personal data. Hence, any collection, storage, sharing, sending or destruction of such data shall be deemed to be the processing of personal data, and is consequentially regulated by the provisions of Slovene law regulating personal data protection[6].

Various studies reveal that some people are afraid that a number of biometric measures could be harmful to their health. In relation to this mention is made of the use of infrared light when screening the retina, or infection problems in relation to fingerprint scans. There are not many such cases in practice. Much more significant is latent data on the health condition of an individual which may be »hidden« within biometric data. Namely, biometric data can reveal much more

than a person may wish to reveal about oneself, or consented to when the collection was carried out. A DNA sample, for example, used to establish the identity of an individual, may also reveal genetic defects and predispositions towards illnesses. Iridologists – scientists who study the characteristics of irises – claim that medical conditions can also be revealed from an iris. A similar situation also exists in relation to voice identification, which may also be used to reveal the emotional state of a person. All these issues are problematic from the perspective of personal data protection. We can also envisage a case in which a company introduces access control by means of the voice recognition of its individual employees.

In November 2009 Mr. Zubair Khan, a Pakistani expert in Biometrics and Privacy presented forgery of fingerprints at Slovene informatics conference Infosek[7]. From point of view of the audience it went very simple: Mr. Khan used some special glue to get (grab) a fingerprint from a glass of wine. When the glue dried, he scanned it in the computer and corrected the scan in Photoshop. After this he printed the picture out of the Photoshop onto a foil. At the end he used some other glue, which he put on the foil-scan and waited to dry. When the glue was dried, he wrapped it around his finger and used it on a biometric reader. The reader recognized the first person, not Mr. Khan's fingerprint.

Today biometrics is a great business – fingerprint readers, iris readers ... are not a part of sci-fi movies anymore, they are part of our everyday life. But just like most of other technologies they support our laziness. You cannot forget your fingerprint at home, as you can in contrast to magnetic or RFID card or keys. You don't have to look for them in a full handbag and they cannot be misplaced. Are you certain about that? With the examples above I dare to conclude that we *can* lose our fingerprints - in a bar for example. They can be stolen – in a way Mr. Zubair showed. They can be abused – just imagine a crime scene where murder was committed and the police find your (forged) fingerprints one step away from the body. What would be your alibi and do you think the police would believe you?

Let me be clear – biometrics is still ok, but just as long as it is under control and it's use is in the framework of the law. As soon as biometric data is collected "just in case we need it" and as soon as we allow the private sector to collect fingerprints, iris scans etc., we can forget about safety. From this moment on we are only a step away from ID thefts. And an ID theft, which was committed with biometric signs, is the hardest to annul.

## Who's watching whom?

Imagine yourself going to the nearest shop. You just want to buy some food, nothing special. You get on the city bus, register your card on a bus card reader and af-

ter the ride you step out in front of the shop. You go inside and wander between shelves. Afterwards you come to the cash desk and scan all your stuff through the bar code reader. There is no cashier at the cash register, since it is automatic. When you scan everything through the automatic reader, it informs you that you bought too much carbon hydrates, because your cholesterol level is too high and that you have to use the condoms you bought 6 months ago because they are about to expire. You are surprised, how much a computer knows about you. But that's relatively harmless, since the ugly truth is that you were under surveillance from the moment you got on the bus.

Actually, in Slovenia the nearest (I hope not) future is only full operating talking computer. Everything else already happened or it could have happened, if Information Commissioner had not prevented it. Let's take a closer look.

The public company LPP, which has the right to manage city public transport in Ljubljana, introduced cards called *Urbana*, which became new means of payment for public transport, parking etc. But this card was collecting the traffic data on a passenger. Passengers gave their consent, but they actually did not have any other choice except giving the consent, since there is only one public transport service - managed by the LPP. That's why Slovene Information Commissioner banned collecting the traffic data.

More or less all shopping malls in Slovenia are equipped with video surveillance, some wants even face recognition system for marketing purposes. So, the procedure is imagined to be something like this: from the moment you step in front of the mall, you are recorded on videotape. Once you are in the mall, video surveillance transforms into face recognition and read your facial features. The system calculates how old you are, finds out your gender and follows your every step in the mall. The system produces (in real time) your path through the mall, which would allow the retailers to redistribute their products to achieve best selling results (Information Commissioner banned face recognition before it was introduced). You pay with your loyalty credit card. The system recognizes your card and calculates what you bought in the past and warns you about expiry dates (part of profiling). Last year one of Slovenia's biggest retail chains introduced such cards and only announced it to their customers. Information Commissioner ordered the company to get new explicit individuals' consents. In Slovenia behaviour loyalty cards are introduced even in pharmacies.

At first sight, it would seem like you are having a simple shopping afternoon, but from the view of the Privacy backend it is huge invasion into individual's Privacy.

I only wonder how far away we are from the moment when we will say that we are not watching TV, but TV is watching us - with commercials adjusted to the viewer.

Another Privacy invasion technology is being developed in Slovenia. Voice recognition by itself is nothing new on the market. What's new is that new voice recognition technology could be used for calling centres, like the police, hospitals and in the second step also in the private sector. The technology would deduce from callers' voice their emotions and – in case of real emergency – transfer the call to the most competent person at the police, hospital ... Up to here I don't see any bigger problems, but the problems will – in my opinion – occur at the moment when this technology becomes a part of the private sector. The private sector will definitely use (or abuse?) it for commercial purposes, which will bring all sorts of new databases, holding Personal Data. Just imagine – you step in the shop and say simple hello to the seller. The voice recognition recognizes sadness in your voice and the commercial board next to you offers you to buy a hanky.

Facts stated above often remind me on the Hollywood movie Minority Report, where Tom Cruise steps into the shopping mall and the system uses face recognition and offers him products he bought in the past. The movie was released in 2002. At that time I think this was only sci-fi. When I read again these lines I think we are only a step or less away from "the past sci-fi".

## Because there is no patch for human stupidity (Kevin Mitnick)

To this point I've been writing about huge databases. But the next issue is how to secure all those data and why the Privacy is so important nowadays.

Can you imagine if 100 years ago the mayor of NY City would have wanted a transcript of the list with all Personal Data of the New York citizens? It would have probably taken several weeks, if not even a year or something. Today the procedure takes about ... a second. The information technology progresses so quickly that even some IT guys cannot catch up with the development in a real time. But the biggest impact of this rapid development is best seen in Privacy Invasion. Who hasn't already "googled" or "facebooked" someone? Who can say he or she hasn't published any Personal Data on the internet (or maybe they were published by others)? I think no one.

But, are we capable of securing all information on the one hand and not (ab-)use published information on the other? Voyeurism is in human nature. Voyeurism in browsing for Personal (and other) Data. Curiosity maybe sounds more polite, but modern internet-sniffing is more like voyeurism. Modern people tend to get as much information as they can and what is more important, they are willing to

pay more and more for good information. Furthermore, they expect to be awarded for disclosing (confidential) information. No wonder social engineers and experts for penetration testing make so much money.

Social engineering is no novelty. Just remember the Trojan horse – classic example of social engineering. But in modern society the social engineering plays a much more important and significant role. Some companies can use millions of dollars to secure their IT system, but this system can be broken just with a few psychological tricks of a cunning man. And this is the biggest risk for Personal Data. In the end there is always and everywhere someone who *has* to press the button. And if this crucial person isn't trustworthy all the IT security means nothing.

The only way to prevent social engineering is by education and honesty. I know it may sound a little bit childish, but I'm totally confident in what I'm saying. If the person who presses the button doesn't have both of them, you spent all that money for nothing.

As stated above – there is still the other side; publishing Personal Data on the internet by a person personally. Actually we cannot do anything if someone is convinced he or she will publish her or his Personal Data. And that is why I chose this title for the chapter.

We must never forget that every right recognized by the law has two very important components – the active and the passive. The active component enables an individual to assert his right, whereas the passive (component) enables an individual *not* to assert his right. So the decision is up to him/her/you. We cannot force someone to exercise his/her right if she or he doesn't want to (except in cases set by the law). So this is one great black hole for social engineers. And, absurdly, at the end it is only the law, which will protect individuals from bad decisions. How this law is implemented in individual countries is another story. But, what I want to stress is that the law should at least theoretically prevent almost all abuses. And if not, the law provides the punishment for an offender and satisfaction for victims/individuals. The line is slippery, but our job is to spread the awareness of Privacy importance. Otherwise we will join those celebrities who feel more or less the same as Princess Margaret who once said: "I have as much privacy as a goldfish in a bowl."

## Endnotes

1. Schneier, On Security 2008 (p. 11) talks about base rate fallacy - that means that some system can make false positive or negative alarms in some database, even if the accuracy is high: »Every day of every year, the police will have to investigate 27 million potential plots in order to find the one real terrorist plot per month. Raise that false-positive accuracy to an absurd 99.9999% and you're still chasing 2,750 false alarms per day – but that will inevitably raise your false negatives, and you're going to miss some of those ten real plots (Schneier, p. 11)."

2. You can read some of Mr. Farouk Umar Abdulmutallab posts on: http://en.wikipedia.org/wiki/Umar_Farouk_Abdulmutallab.
3. http://www.youtube.com/watch?v=nrKvweNugnQ.
4. Very important issue at this point is to consider the possibility of Data Pollution – read more: http://www.parasoft.com/jsp/aep/aep_practices.jsp?practice=DataPollut.
5. http://en.wikipedia.org/wiki/DNA_profiling.
6. Read more: http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Guidelines_biometrics.pdf.
7. http://www.infosek.net/.

# Biometrics, e-identity and the balance between security and privacy-the case study of Passenger Name Record (PNR) system

George Nouskalis

## Introduction

The implementations of biometrics entail either the establishment of identity or the tracing of a person's identity. Biometric passports (iris, finger, face e.g.) can be used in order to verify the passenger's identity. The published proposal of European Commission for a Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, specially combating terrorism, raises security and privacy issues, which become more complicated due to the use of the above e-passports.[1]

The proposed PNR record contains all information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person. PNR data are related to travel movements, usually flights, and include passport data, name, address, telephone numbers, travel agent, credit card number history of changes in the flight schedule, seat preferences and other information. The collection and analysis of PNR data allow the law enforcement authorities to identify high-risk persons and to take appropriate measures.[2]

In the aftermath of September 11, a new emergency political-law status of the society is established: the continuous state of "war" against the so-called unlawful combatants of the "enemy". Officially the enemy is the terrorists although the victims of the privacy invasions through the above new form of data-processing are civilians. The problem is that some measures against terrorism, for example an excessive data-processing system as PNR, may seem reasonable in a situation of war although they would never be acceptable in a time of piece. However, there is a tension between addressing terrorism as a crime and addressing it as a war.

The combination of the above PNR date and the system based on biometrics, i.e fingerprint or iris or recognition in passports provoke with both new challenges and thinking about the balance between security and privacy. The condition for giving a visa permission and the asylum policies are also relative matters. This paper attempts to clarify the main aspects of this subject and to bring into question the compatibility of the above biometric PNR data base with the proportionality

principle, which is fundamental in the processing of personal data in accordance with the Directive 95/46.

## The legal framework

Data-processing based on biometrics is covered both by the Directive 95/46 E.C and Art. 8 of the Convention on the Protection of Human Rights and Fundamental Freedoms (hence " ECHR"). According to Art. 2 par. a of the above Directive personal data is any information relating to an identified or identifiable natural person. 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. In accrordance with Art. 8 of ECHR, everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and it is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Respect for private life also consists of a the right to establish professional or business relationship[3]. It is certain that also public information falls within the scope of private life when it is systematically collected and processed in files held by the authorities. The ECHR has emphasised the correspondence of this broad interpretation with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, such personal data being defined in Article 2 as "any information relating to an identified or identifiable individual".

The provisions of this legislation constitute a concrete framework based on the following structure: the rule is that processing is lawful when data are processed fairly and in an adequate, relevant and not excessive way in accordance with Art. 5 of the Directive. Although a binding international agreement between the EU and the US on privacy and data protection, in the context of the exchange of information for law-enforcement purposes, remains of the utmost importance, the EU seems to realize the necessity of a core of privacy-island in the middle of the processing "ocean" .

The above proposed Framework Decision provides for the transfer or the making available by air carriers of PNR data of passengers of international flights to the Member States, for the purpose of preventing, detecting, investigating and prosecuting "terrorist offences or serious crime.[4] In accordance with Art. 5 of the Directive personal data should be collected for specified, explicit and legitimate

purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member-States provide appropriate safeguards". In the EU data protection legal framework the before mentioned provisions generate the purpose specification princinple. The purposes for which data are collected should be specified not later than at the time of data collection and the use of the data should be limited to the accomplishment of those purposes. The breach of that principle constitutes an unlawful processing of personal data.

In the explanatory report of the above proposal it is mentioned that the scope of the proposal is limited to those elements which require a harmonised EU approach.[5] However, there is no certain limitation about the extent of the collected data of so many people, who are not officially either suspect or accused for any crime. Proportionality is often raised in general terms, without further explanation. The most critical question which relatively arises is the meaning of the proportionality principle and which factors are taken into account.

The principle of proportionality is a very important factor in the legal review of biometric systems. The question that arises is related with the specific criteria and factors used for evaluating the proportionality of processing biometric information. The application of the proportionality principle requires a certain duration of processing and a limited area of felonies which can be investigated through the collection of PNR data. According to the above proposal, data is to be kept for five years, which constitutes rather a disproportionate invasion of privacy in order to fight uncertain threats, if somebody takes into consideration that these data can be used for other purposes beyond fighting terrorism or serious criminality. It should also be noted that the general invocation of terrorism or serious crimes does not fulfil the requirement of purpose specification. There should be further clarification of the reason for the processing of the data.

## The new legal notion of privacy in a postmordern context of continuous fight against terrorism and serious or organised crime

The interaction of a person with others, even in a public context, may fall within the scope of private life in accordance with the case law of the ECtHR[6]. The emergence of a surveillance society has modified the above public context in order to strike a new balance between security and (social) privacy. A postmodern approach to human rights attempts to set a new paradigm for protection of privacy based on a non-exceptional but continuous state of war against terrorism and organised crime. The question that arises is about the new criteria of interpreta-

tion of proportionality principle in order to establish a new legal doctrine about the extension of measures restraining privacy.

This biometric technology creates new ethical issues of the so- called surveillance society. One of them is the impact on privacy. The thinking about proportionality of the related constraints in privacy is based on a reversed rule: the collection, storage and processing of PNR biometric data constitute a necessary measure to safeguard security under EU data protection law. Today the above processing is not the ultima ratio of data protection law based on fighting against criminals, however a proper process through which a structure of security can be ensured. This acknowledgment implies some thoughts about justification of the related impact on privacy. In other words the legally-considered invasion of privacy can be acceptable when the relevant data processing is the necessary measure to protect society from terrorism or serious crime. The result is that there is a proper ratio between the two above components.

The enhancing of security in order to assist criminal law enforcement agencies through the above PNR system constitutes a new, postomodern, Panoptikon,[7] as it is described sociologically in terms found in the work of Michel Foucault[8]. The majority of the people can be considered as suspects of crime through the collection, storage and processing of the above PNR data used by law enforcement agencies based on the invalidation of the presumption of innonence, in a permanent state of exception. In this context the majority can be accounted as internal and unlawful combatants of the enemy in a war between a State and their citizens[9]. Thus, a legal framework based on the exceptional processing of personal data can not adjust to the new rule of collection, storage and processing in order to fight terrorism and serious crime.

## Conclusions

The published proposal of European Commission for a Framework Decision on the use of (PNR) data for law enforcement purposes raises security and privacy issues in a postmodern era, which could entail a wide interpretation of a justification of the above data processing based on the continuous fight against terrorism and serious crime. The provisions of the EU data-protection law based on the exceptional processing of data cannot imply in the new environment in which the majority of the people are considered as suspect of crime.

## Endnotes

1. See T E. Brouwer, The EU Passenger Name Record System and Human Rights Transferring passenger data or passenger freedom? CEPS Working Document No. 320/September 2009, http://www.ceps.eu.
2. See .H. Tielemans, K Van Quathem D.Fagan A. Weber, Personal Data The Transfer Of Airline Passenger Data to the U.S.: An Analysis of the ECJ, http://www.cov.com/files/Publication/8aa81e95-460a-4d30-a901-28b14757ec00/Presentation/PublicationAttachment/37f11b14-ff49-4e95-a5ce-2ee016f94329/oid23778.pdf Decision.
3. See the Niemietz v. Germany judgment of 16 December 1992 decided case of ECtHR, http://webcache.googleusercontent.com/search?q=cache:YYgLG8pY_e4J:www.bartosz-bilinski.pl/hr/case_of_niemietz.ppt+see+the+Niemietz+v.+Germany+judgment+of+16+December+1992&cd=1&hl=el&ct=clnk&gl=gr.
4. F. Aarts J. Schmaltz F. Vaandrager, Inference and Abstraction of the Biometric Passport http://www.mbsd.cs.ru.nl/publications/papers/fvaan/passport/.
5. See at http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l14584_en.htm.
6. See P.G. and J. H. v. the United Kingdom, no. 44787/98, §§ 56-57, ECHR 2001 IX.
7. See A. Albrechtslund, The Postmodern Panopticon: Surveillance and Privacy in the Age of Ubiquitous Computing, available at http://albrechtslund.nlt/texts/postmodernpanopticon.pdf.
8. M. Foucault, Discipline and Punish: The Birth of the Prison, 1975.
9. See N. Chomsky http://www.counterpunch.org/chomskyterror.html, P.Swire http://www.counterpunch.org/swire1.html.

# The right of access to information in Mexico

**Oscar Mauricio Guerra Ford**

## Transparency in Mexico

The right of access to information in Mexico was established for the first time in the Federal Constitution reform made back in 1977, when the Sixth Constitutional Article was amended by adding ten words: "The right to information is guaranteed by the State". Since then, this right has been recognized as a fundamental right in the Mexican Constitution.

In 2002, after the publication of the Federal Transparency and Access to Public Information Act that created the first organism in charge or guaranteeing the right to access to information (IFAI), many states as well as the Federal District began to create their acts on access to information, along with the creation of organisms to guarantee the exercise of this right.

In this context, in2006, 31 states, the Federation and the Federal District, already had specific laws on access to information and agencies to ensure this right, and to monitor the compliance of the law. In this first stage, only four states did not have an Authority to watch over this right: Aguascalientes, Jalisco, Tamaulipas and Veracruz.

The first years of practice of the right of access to information presented a series of failures caused by the heterogeneity of the Acts:

Most Acts established a set of requirements counteracting the right of citizens to obtain public information (obligation to affix signature in information requests and complaints with regards to given answers, accreditation of personality through the presentation of an ID, failure to submit applications electronically), or in some cases there was no agency where citizens could address their complaints with regards to the given answer to a request, or in the case where they did not received a response from the public entity. Finally, if there were any, agencies were not proficient to make this right effective as far as the attention of complaints was responsibility of other bodies, mostly within the judicial branch.

These deficiencies impelled further reforms to article 6 of the Federal Constitution, mostly because the disparity in the exercise and protection of the right of access to information from one state to another was unacceptable.

Consequently, in July, 2007 seven fractions were added to this article in order to include a set of principles under which this right should be guaranteed.

The latest reform emphasized the importance of three major issues: access to information, personal data protection and public records, establishing the following obligations:

- All information held by any authority, institution, body or federal agency, local and municipal, is public and can only be reserved temporarily for reasons of public interest in terms of the legislation. In the interpretation of this right the principle of maximum disclosure should prevail.
- Everyone has free access to public information, to personal data (or to correct it) through the set up of prompt mechanisms to access information and reviewing procedures, to be substantiated by specialized autonomous impartial agencies with autonomy (freedom to spend its own budget, and to determine its management procedures and decision-making processes). In all cases these agencies should protect the information related to privacy and personal data in the terms and exceptions established by the appropriate law.
- All public entities should protect and guard its documents in actualized administrative records, and have the obligation to publish in their websites, comprehensive and updated information on their performance, along with indicators and their public resources accountability.
- The laws should determine how the information about public resources delivered to public or private institutions or entities should be disclose.

These amendments implied two obligations: 1) To modify the existing Acts in a term no longer than one year after the publication of the amendment, in order met the requirements set in the Constitution; 2) To establish electronic systems to make easy the access to information (this system would be available two years after the publication of the amendment).

It also included basic principles such as: all information possessed by public bodies of the Mexican state is public, with the only exceptions provided by law; information made public is subject to the principle of maximum disclosure; citizens have the right of Habeas Data (protection of privacy, right of access and correction of personal data); there is no need to prove legitimated interest, or to justify the use of the requested information and finally, public information is free, except when the documents holding the information must be reproduced.

The main objectives of this reform were:

a. Establish expedited procedures to access information and the mechanisms of attention of complaints. To do so, it was necessary to implement electronic systems for the presentation of information requests in order to break with the tradition of receiving applications in person at the Offices of Public Information (OPI's).

b. Establishment of specialized and impartial guarantor agencies with operational, budgetary and decision making autonomy:

   Agencies in charge of safeguarding the right to access information must have certain characteristics. The first one is specialization, which ensures that decision makers have the necessary expertise to adequately assess arising cases. The second element is impartiality, to ensure that both the integration and operation of the bodies or agencies will not respond, directly or indirectly, to authority bodies and act professionally and objectively.

   To achieve this, the reform established that transparency organisms should have three types of autonomy aimed to ensure impartiality and specialization: operational freedom which means that the organism is responsible for its own administrative criteria; budget management freedom, this is, the organism should be able to approve projects from the budget assigned to it and exercise it based on the principles of effectiveness, efficiency and transparency, considering at all times the specifications set by the Law, and also being able to authorize changes and determine the corresponding adjustments in its budget. Finally they must have freedom of decision, which involves a law-based performance and independent judgment capacity duly founded and motivated, regardless of the authorities in charge.

c. Obligation for all public bodies to publish their performance indicators.

d. Obligation to have up to date and reliable administrative archives that allow the easy location and the release of information.

e. Publication of information on public resources.

f. Establishing penalties in case of failures in the compliance of the law.

Three years after this reform, 23 laws comply with the provisions of said Constitutional article 6 and 9 laws do not (including the Federal Law). Likewise, only 12 states have constitutionally guaranteeing-autonomous bodies, (autonomy derives from the constitution of each state), 18 are autonomous and two states (Baja California and Sonora) and the Federation do not have autonomous bodies.

Within the group of laws that do not meet the new content of article 6 we have 3 cases: The laws of the states of Puebla, Campeche, and Queretaro.

These cases are being reviewed by the National Supreme Court of Justice in order to declare the unconstitutionality of the rule but this has happened only in the case of the Querétaro Act.

Particularly, in the case of Puebla, the Act provides that the Guarantor Authority, named Commission for Access to Public Information of the State of Puebla (CAIP), has jurisdiction only over the executive branch and not over the municipalities, obligating each of them to create municipal authorities. This interpretation constitutes a violation of the Constitution due to the fact that it establishes a unique guarantor body for each state with broad competence over all its municipalities.

The law of the state of Campeche was amended establishing that attention of complaints regarding unacceptable replies to requests would be issued and solved by a judicial body, action contrary to what is established in section IV of article, stating that all procedures regarding access to information must be issued and solved by specialized agencies. In this sense, if the rule provides that the guaranteeing transparency body is the only organisms specialized on this topic, the review function cannot be placed in any other institution.

Finally, the Queretaro state law was amended to incorporate the functions of the guaranteeing transparency body to the Human Rights State Commission in order to create a single agency responsible for two different tasks.

The National Supreme Court of Justice declared Article 33 of the Constitution of the state of Querétaro to be unconstitutional, therefore it was amended to provide that functions of safeguarding the right to access information would fall only into one specialized agency in the matter, according to fraction IV of article 6 of the Federal Constitution.

Although there have been many improvements that allowed a growing trend on the exercise of these rights, yet there is much to do. One of the most important points still pending in the Constitution is the recognition of the fact that resolutions emitted by the guarantor bodies are final and definitive because, as it happens in the state of Campeche, today there are many legislative projects seeking to limit this right through the review of resolutions issued by these organisms, which, no doubt, given the Mexican political and social context, would diminish and subsequently deny the exercise of the rights.

## Transparency in the Federal District (Mexico City).

Four years after the foundation of the Institute for Access to Public Information of the Federal District (InfoDF), as guarantor of the right to access public information in the Federal District, it can be categorically stated that citizenship is increasingly obtaining information of public institutions of the nation's capital, as an effective measure of their effort to participate in public affairs that will lead them to a better life quality status.

Achieving this goal implied for InfoDF the consolidation of objectives and overcoming challenges and weaknesses characteristic of a political and administrative system that begins in the practice of delivering and providing public information about the distribution, use and destination of public resources.

Enhancing transparency as a transforming agent of the relationship between citizens and the state has been a priority for InfoDF. The willingness of citizens to obtain public information by any lawful means must be reflected in the integrity of public servants. Therefore, we have monitored the information posted in websites and given to applicants to be timely appropriate and accurate. These actions contribute to empower citizens in order to influence public policy.

Dynamism on the regulations governing access to public information in the Federal District is a sign of the strength they have acquired due to two transverse demands of citizenship: accountability and the protection and preservation of information withheld by public institutions. Since the publication of the original legislation in 2003, there have been many reforms in sought to consolidate the right to access information and protection of personal data.

In July 2nd, 2007 with the amendment to Article 6 of the Constitution the institutional framework supporting the right to access public information became stronger. As a result of this dynamic process the new Transparency and Access to Public Information of the Federal District Act (T&ATPI Act), on March 28th, 2008, the Personal Data Protection Act for the District Federal (PDP Act.) on October 3rd, and the Archives Act of the Federal District on October 8th were published.

The new T&ATPI Act introduces new elements in transparency:

1. Specific obligations to publish information on Internet websites were established for government agencies.
2. It recognizes the possibility to submit information requests by telephone; also, different deadlines were established to attend information requests: 10 days for public information and 5 days for information published in their websites.

3. The period to attend complaints with regards to given answers was reduced to 40 days or less. If the action is brought as a result of the non replying of inquiries for information, the deadline to issue a resolution is 15 days;

4. New entities are bound to the compliance of the law (the number grew up from 83 to 146): among others, 14 political associations, 8 decentralized, deconcentrated and auxiliary authorities and 8 political parties were incorporated.

5. General obligations were established for all public entities and in addition, the Act sets specific obligations for each type of branch. General obligations include the following:

   - Article 13: Obligation to publish catalogs of public information in accordance with the general filing archives.
   - Article 14 requires the publication of 27 items, among we find: budget information, staff, bidding, purchasing and procurement, regulatory framework, directories, functions, organization, information on social programs, etc.
   - Article 28: Standards to publish public information.
   - Article 29: Obligation to publish calendars for the updating of information.

6. Transparency obligations are set specifically to the Executive, Legislative, Judicial and Autonomous institutions:

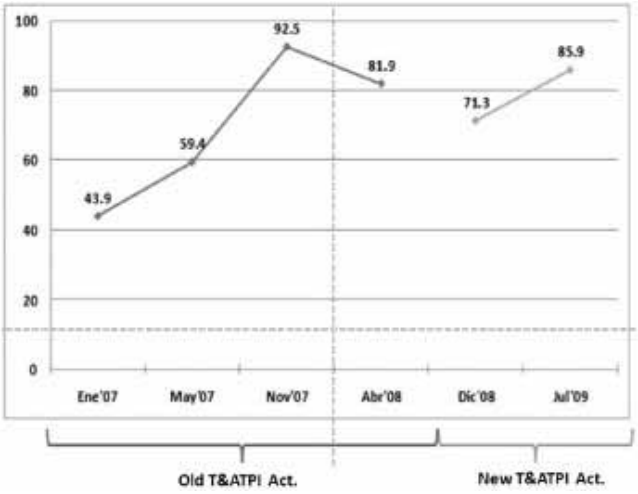
   - Executive (art. 15) 10 obligations, crime rate statistics and law enforcement indicators, statistics on previous inquiries, arrest warrants.
   - Judicial (art. 17). 25 obligations outstanding issued resolutions, agreements, and the legal newsletter.
   - Electoral Institute and Electoral Tribunal (art. 19). 13 obligations, including: election results, electoral territorial division, notes and resolutions of the plenary, legal resolutions and results of the audits practiced to political parties.
   - Human Rights Commission (Art. 20). It establishes3 obligations including public versions of the recommendations and statistics of their duties.
   - InfoDF (art. 22). It contains 8 obligations including: Plenary resolutions on complaints with regards to given answers, results of evaluation and promotion of the right to access.

7. Any person may file a complaint at the InfoDF when this information is not being correctly published, nor completely (Art. 14). The institute has to solve the complaints in 15 working days.

Due to the greater accuracy and high standards established in the T&ATPI Act for information published in websites, many improvements can be observed in

the quality of this information, such as in the compliance of their transparency obligations.

**Graphic 1**
**Total scores average on information published in websites**




**Source**: InfoDF, Evaluation and Studies Department.

## Advances in the exercise of the right to access to public information

Since its creation in 2006, InfoDF evolved as the institution in charge of watching over the right to access public information. In 2008, the PDP Act allocated the same task regarding protection of personal data held by public bodies. With this new mission the Institute acquired a public commitment of unquestionable relevance in the construction of democracy and in the protection of the rights of citizenship.

The first four years were devoted to establish conditions and institutional procedures necessary to ensure a solid foundation of these rights in terms of regulations, technological treatment and to procure services.

At that time the Federal District was the first federal entity to adopt the electronic system named Infomex (electronic platform created by the IFAI), an electronic filing and responding system to attend information requests.

Also, considering that in Mexico only 13.5% of people has access to Internet, while 51% has telephone service from a landline and 61% from a cellular phone, InfoDF implemented a mechanism called "Tel-InfoDF", where you can submit information re-

quests by phone. It also established a SMS notification service, useful to citizens who submitted information requests via Infomex. This way, they will receive notifications about the status of their request, after providing their cell phone number in Infomex.

With these three mechanisms the access to public information becomes easier for people interested in exercising their right to be informed, because they do not need to go personally to the OPI's to present their applications.

As shown in the table below, the implementation of electronic systems to present information requests ranked first with a 54% of the total. Alongside in 2009, 40% of the information requests were submitted through the Tel-InfoDF system:

**Table 1**
**Presentation of information requests**

| Tools | 2006 | 2007 | 2008 | 2009 |
|---|---|---|---|---|
| INFOMEX | 13.2% | 57.9% | 57.5% | 54.0% |
| TEL-InfoDF | | 13.4% | 29.2% | 40.0% |
| E-mail | 32.6% | 10.6% | 4.6% | 2.0% |
| Personally in OIP'S | 51.3% | 17.5% | 8.7% | 4.0% |
| Other | 2.9% | 0.6% | | |
| Total | 100% | 100% | 100% | 100% |

**Source**: InfoDF, Evaluation and Studies Department.

Corruption and impunity weaken public and private institutions, distort our economies and undermine the social moral. The responsibility for the prevention and control of these problems lies in all branches of the local government, with the collaboration of society as a whole. By delivering government information to society, the number of guards increases; it enhances their capacity to assess and empowers people to identify actions that fall outside the established legal parameters.

Strengthening democratic governance calls for overcoming poverty and promoting equitable economic growth through public policies and good governance practices that promote equal opportunities, education, health and full employment. Thus providing citizens the tools to avail from information enables them to effectively exercise their rights and it is also essential for making informed business decisions and to create strategies to influence public policy through society's active participation.

In this context the right to access public information is of great importance, especially in those sectors of society that do not have information to make decisions that significantly affect their quality of life. For this reason, since 2008, the InfoDF defined as a priority the extension of knowledge of the right to access

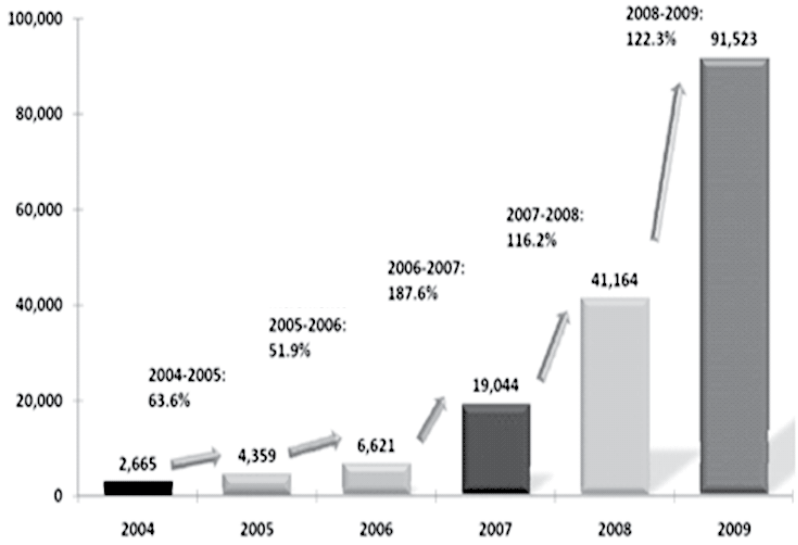
public information in order to encourage the participation of citizens in the consolidation of a democratic system.

With the aim of broadening awareness of the right to access public information, mass communication strategies were established through alternative media channels to launch, with a low expenditure, the transparency message to more people.

Special attention was also paid to promote this right trough the creation of a specific Department in the Institute expressly created to contact citizens directly to inform them of their rights. In these sense, face to face dialogues with civil society organizations and public authorities take place every day to promote social participation.

These efforts, combined with the media campaign, as well as alternative marketing strategies and relationship to society, allowed to increase significantly the number of applications as shown in the chart below.

**Graphic 2**
**Total Information request from 2004 - 2009: 165,376**




**Source:** InfoDF, Evaluation and Studies Department

The increase in the number of information requests was possible due to the promotion strategy and the implementation of two mechanisms: the Tel-InfoDF system and the SMS service. As a result, other sectors of society were incorporated to the exercise of the right to access public information:

**Table 2**
**Applicants' occupation**

| Ocupation | 2007 | 2008 | 2009 |
|---|---|---|---|
| | % | | |
| Academic/Student | 15.9 | 10.5 | 30.2 |
| NG0's | 4.3 | 4.2 | 2.4 |
| Media | 24.3 | 14.5 | 4.0 |
| Public Servant | 9.3 | 2.4 | 11.8 |
| Political Association | 1.4 | 1.3 | 1.1 |
| Employee/Worker | 9.9 | 36.7 | 19.2 |
| Merchant | 4.4 | 5.3 | 6.8 |
| Entrepreneur | 3.3 | 1.6 | 6.4 |
| Home | 0.9 | 2.4 | - |
| Other | 26.4 | 21.1 | 18.3 |
| Total | 100 | 100 | 100 |

**Source:** InfoDF, Evaluation and Studies Department

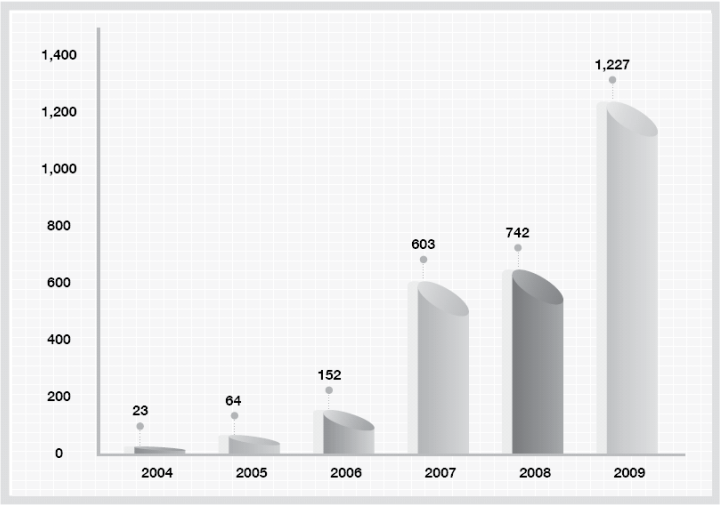
Moreover, as a mechanism to guarantee the exercise of this right, citizens have the possibility to appeal the responses received by public authorities. Trough this mechanism, InfoDF reviews that the response was emitted according to the principles established in the Law, to ensure that citizens acknowledge legal, verifiable and public information.

This function is carried out through the resolution of appeals which derived from a procedure in the form of trial, the Plenum of the Institute determines to confirm, revoke or modify the reply of the public body when the disagreement stems from the response issued or, ordering the public body to issue a response to the information request when request of information was non replied.

Placing monitoring and control mechanisms into society encourages greater compliance of the law. This is evidenced by the multiple appeals for review solved by this Institute where citizens were able to obtain information about construction of buildings, social defense programs, licenses of various commercial establishments, environmental impact studies of a variety of public works and information on market inspectors and supervisors. In all these cases citizens learned how information helps effectively to protect and exercise other rights.

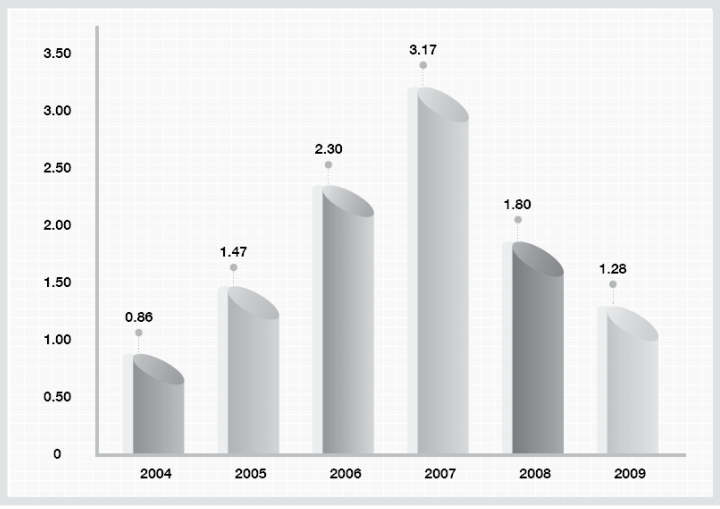
Although the number of appeals for review filed has increased, the relative terms we see that there are fewer applicants unsatisfied with the answers to their requests.

**Graphic 3**
**3.1 Appeals for review presented to InfoDF per year**




**Source:** InfoDF. Legal and Regulatory Development Department & Technical Secretariat.

**3.2 Percentage of information requests that turned into appeals for review**




**Source:** InfoDF. Legal and Regulatory Development Department & Technical Secretariat.

InfoDF guarantees the right to access public information by strengthening the processes of substantiation and resolution of appeals for review presented by applicants in terms of the T&ATPI Act. This action reflected a reduction in the resolution time: it went from 41.9 days in the first quarter of 2008 to 31.8 days in the last quarter of that year.

By resolving these appeals the Institute seeks to maintain a healthy balance between the protection of personal data, protection of confidential information and the principle of maximum disclosure. In table 3 you can see how the Institute has solved these appeals.

**Table 3**
**How do appeals for review are solved**

| Resolution | 2007 | | 2008 | | 2009 | |
|---|---|---|---|---|---|---|
| | Number of Appeals for Review | % | Number of Appeals for Review | % | Number of Appeals for Review | % |
| **Plenary resolutions** | 358 | 69.2 | 476 | 63.3 | 662 | 60.8 |
| Confirm | 33 | 6.4 | 81 | 10.8 | 91 | 8.4 |
| Modify | 126 | 24.4 | 155 | 20.6 | 242 | 22.2 |
| Revoke | 88 | 17 | 119 | 15.8 | 109 | 10 |
| Confirm omission to respond | 55 | 10.6 | 66 | 8.8 | 99 | 9.1 |
| Dismiss | 56 | 10.8 | 55 | 7.3 | 121 | 11.1 |
| **Solved by Agrements** | 159 | 30.8 | 276 | 36.7 | 427 | 39.2 |
| Dismiss | 32 | 6.2 | 42 | 5.6 | 38 | 3.5 |
| Discarded as inadmissible | 26 | 5 | 104 | 13.8 | 198 | 18.2 |
| Not Presented | 101 | 19.5 | 130 | 17.3 | 191 | 17.5 |
| **Total** | **517** | **100** | **752** | **100** | **1089** | **100** |

**Source:** InfoDF. Legal and Regulatory Development Department & Technical Secretariat.

Moreover, since its creation InfoDF has taken inter linkage actions with public entities and universities, with civil society organizations and with national and foreign counterparts in order to create conditions that will encourage greater disclosure and use of the right to access public information, which allows to form a common knowledge among public servants and civilians interested in the subject.

Since 2007, InfoDF has implemented correlation policies with the society to promote awareness and exercise the right to access public information, including general population and civil society organizations. This policy aims to enhance the impact of promoting the right to access public information that is made by other means, while generating social knowledge in order to evaluate and monitor the performance of local public institutions and, to the extent of their possibilities, the opportunity to influence the design of public policies.

The specific mechanism to achieve this goal has been the strengthening of relationships with Non Governmental Organizations (NGO's) and in the implementation of face to face activities with the general population.

On this matter we can highlight four actions that were implemented to link society with the right access public information: Social Participation Programs, Roundtable for Transparency, the 1st Transparency Fair and various International Seminars were new contributions on focalized transparency were made.

The Social Participation Program is divided into two categories: the first one called "General Population" includes the making of promotional events in political communities, educational institutions, public agencies, academic and cultural events, talks and brochures distribution on the streets (action also known as the Transparent Wave) and specialized care centers (PAC).

The second item called "Organized Civil Society" InfoDF has invited the NGO's to become strategic players in the development of the right to access public information and in strengthening the culture of transparency and government accountability within society. This line of work seeks to build bridges between the Institute and marginalized groups in the City to use this right to solve specific social problems and to improve their quality of life.

NGO's participated in this effort trough the presentation of projects financed by various social programs and supervised by the Institute with the aim of promoting the right of access to information as a tool to get a better quality of life.

The Roundtable on Transparency in the Federal District was formed in 2008, an initiative of InfoDF to procure a mechanism for the exchange of ideas and the analysis about the status of transparency in public institutions, and as a space for agencies to generate strategic agreements to promote the culture of transparency and accountability in the local level. Alongside with InfoDF, the actors involved in this project are public entities representatives, NGOs and other bodies of the capital's society (academics, journalists, trade unions representatives, political groups, businessmen, etc.)

There have been four roundtables where there was an approach to topics of Public Safety, Environment Transparency and in policies and social programs of the Federal District. This mechanism has proven to be an articulated strategy of effort between authorities and citizenship that has improved the dialogue between suppliers and demanders of information, has increased the impact of policies on transparency, makes simpler the language of the information published on the government, created websites with relevant information, it has improved organized civil society capacity to influence in public policies, etc.

Furthermore, as an unprecedented event in Mexico and with the participation of 60 public bodies, 14 civil society organizations and 9 transparency guaranteeing bodies, on Monday, September 28, 2009 the 1st Transparency Fair took place on the main square of Mexico City, an event that brought together more than 10 thousand attendees. This event was made to commemorate the Right to Access Public Information International Day adopted in Bulgary in 2002 with the purpose of recognizing the importance of this fundamental right in democratic life, and encourage countries to adopt measures to combat and overcome the obstacles that hinder this right.

Public bodies and NGO's that participated in this event provided attendees with information on the practice of transparency and access to public information within their respective responsibilities and areas of interest. Allusive materials were distributed to invite citizens to become aware of the importance of knowing and exercising this right.

During the development of the Fair different cultural and leisure activities were held such as a Puppet Theater, flamenco dancing, a theater play called *The Crystal Circus* was performed and there was a chance to *score a goal* against corruption. In addition, clinical services were offered (mammography), talks by the Heroic Fire Department and an orientation module from the Ministry of Finance were established to clear up doubts and inform about services provided by it.

This event allowed spreading among citizens, the knowledge about all social benefits of using and practicing the right to access public information, transparency and accountability.

Finally, in the framework of the 3rd International Seminar *Towards a New Generation of Transparency*, there were several tables of analysis in order to know and reflect on new trends in the policies of transparency and access to public information, in the search to provide greater social benefit, and the role they play in them the technological tools and the social and political actors.

Finally, it is important to highlight the contributions on focalized or pro-active transparency as a mechanism to respond to the need for specific benefits. As well as the demand for a more organized and useful information posted in government web pages.

## Personal data protection

With the enhancement of the Personal Data Protection Act, the Institute implemented specific regulations to ensure proper protection of personal data and verify the application of the so-called ARCO rights: access, rectification, cancellation and opposition.

In this context, since October 14th, 2009 the Federal District has general guidelines on how data should be collected and processed to facilitate the execution of ARCO rights and to ensure that data will only be used for lawful purposes under security measures that will guarantee its confidentiality.

Also an electronic registration system of personal data systems was developed to facilitate the updating of the information currently contained in the Institute's register of personal data systems.

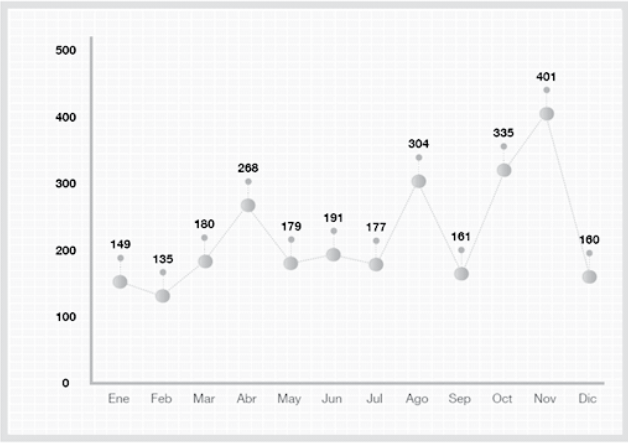
The development of the right of access to public information since 2004 has opened a way to exercise the rights of protection of personal data with its own characteristics and dynamics.

In this regards, in 2009 requests for access, rectification, cancellation and opposition of personal data (ARCO applications) reached in the Federal District a total of 2640 and over 75 percent of them were made through the Infomex System.

This result implies an increase of 157 percent over the ARCO applications received in 2008 (1024). Moreover, this result also represents 2.8 percent of the information requests received in 2009 (91,523 applications), a positive change compared to the year 2008, where ARCO applications represented only 2.5 percent of them.

The following chart shows the intensification of applications in the second half of 2009, a period in which 1538 ARCO applications were made. This represents 58.6 percent of all the applications received. The incidence was evident in the months of August, October and November, where 39 percent of the applications were issued.

**Graphic 4**
**Information request growth per month in 2009**




**Source:** InfoDF, Evaluation and Studies Department

Of the four rights protected by the PDP Act, lead the exercise of personal data **access**, with 98.8 percent of the 2640 ARCO applications. While the exercise of rectification, cancellation and opposition the rights was marginal accounting only 1.3 percent of the applications, as shown in the following table:

**Table 4**
**ARCO Rights exercised**

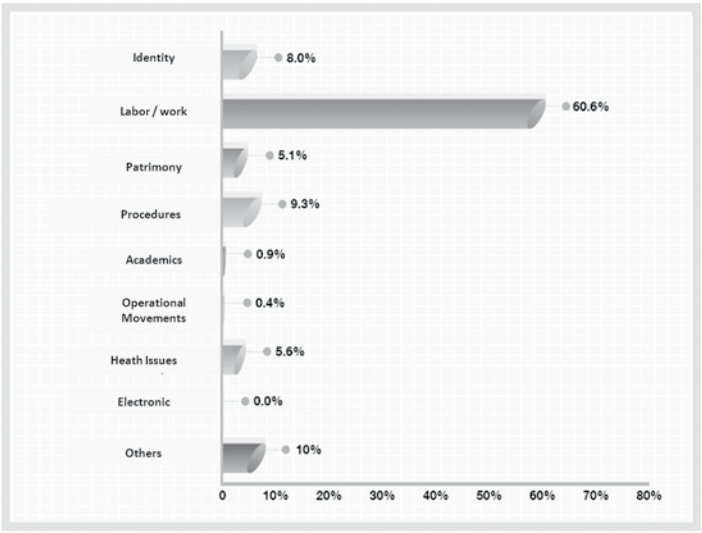
| ARCO rights exercised | Applications received | % |
|---|---|---|
| Access to Personal Data | 2,607 | 98.8 |
| Rectification of Personal Data | 21 | 0.8 |
| Cancelation of Personal Data | 5 | 0.2 |
| Opposition to Personal Data | 7 | 0.3 |
| Total | 2,640 | 100 |

**Source:** InfoDF, Evaluation and Studies Department

The analysis of ARCO applications is complemented by considering the categories of personal data requested. Graphic 5 shows that the predominant category was access to labor data, with 60.6 percent of the applications (1601 applications for a total of 2640), followed, regardless of the category "Others", for the category administrative procedures data (with 264 requirements) and identification data (with 246 applications), representing 9.3 and 8.0 percent of the total, respectively.

Making a cross reference exercise of this information with the information about applicant's profiles, it can be stated that most of the requirements came from public servants who wished to access personal data, contained mainly in labor-type files. (Please check Graphic 6 )

**Graphic 5**
**Category of personal data required by ARCO applicants**




**Source:** InfoDF, Evaluation and Studies Department

**Graphic 6**
**Applicants Profile**

| Occupation | ARCO Applications | % |
|---|---|---|
| Entrepreneur | 8 | 0.6 |
| Media | 1 | 0.1 |
| Merchant | 33 | 2.6 |
| Public servant | 1079 | 84 |
| Academic / Student | 33 | 2.6 |
| Employee / Worker | 64 | 5 |
| Political association | 2 | 0.2 |
| Home | 16 | 1.2 |
| Other | 49 | 3.8 |
| **Total** | **1285*** | **100** |

**Note:** only 1285 applicants answered the socio-demographic data base in Infomex.

**Source:** InfoDF, Evaluation and Studies Department

Unlike requests to access public information, where the delivery of information / resolution can be accomplished by various means, including electronic and Infomex system, in ARCO applications the delivery of the response emitted by the authority can only be made and delivered by the OPI's, after the applicant or legal representative have accredited its personality. For this reason, even when the notifications can be made by any mean (e-mail, Infomex, etc.) they will only have to inform whether or not the application was suitable or not.

This condition of delivery ensures that only the person concerned, or his legal representative, will have legitimate access to information concerning his privacy.

The PDP Act is the legal instrument that ensures the protection, guard and proper use of individuals' personal data held by public bodies in Mexico City. As already indicated, the PDP Act acknowledges and grant access, rectification, cancellation and opposition of personal data rights.

The rule provides that in case these rights are violated, the persons concerned may present an appeal to the InfoDF, institution in charge of guaranteeing the PDP Act.

In this regard, in 2009 there were 31 appeals against the answers given by 16 public organizations, which represent 1.2 percent of the 2640 ARCO applications.

At the end of 2009, InfoDF's Plenum adopted 16 appeals resolutions related to ARCO requests. Of these, 14 were presented in 2009, while the other two were left unresolved in 2008.

Of the 16 appeals determined, two were filed because there was no reply to the request (RR.937/2009 and RR.031/2009), and the remaining 14 by dissatisfaction with the answers given by public bodies. It is noteworthy that only one resource (RR. 734/2008) was filed on an application for cancellation of personal data, while the remaining 15 were related to requests for access to personal data. Thus, we conclude that, in 2009, there were not appeals by dissatisfaction with the response related to the exercise of the rights of correction and opposition of personal data

Additionally, InfoDF's Legal and Regulatory Development Department resolved 8 appeals due to the fact that public bodies did not comply the formalities laid down in the Act for its procedure.

In compliance with the PDP Act, InfoDF acquires a dual role. First, is the body liable for supervising and monitoring its compliance and on the other hand, it must fulfill its requirements like everyone other public entity. For this reason, in addi-

tion to satisfying the obligations established in the PDP Act, the Institute develops several activities to promote greater awareness and observance of the Law.

The protection of personal data is a topic of recent treatment in the Federal District. In addition to the training activities undertaken by the InfoDF, the activities of public bodies, related to compliance with the provisions of PDP Act, were accompanied in 2009 by providing personal advice to the personal in charge of the of the OPI's and Systems of Personal Data; telephone consultations, meetings with public bodies and conferences on focalized topics.

Training public servants responsible for the Systems of Personal Data is a strategic task in addressing and overcoming the problems detected in the protection and treatment of this type of information. It is important to emphasize that for the first time, the training provided on the contents of the PDP Act, include an additional content on the Guidelines for the Protection of Personal Data in Mexico City, a complementary legislation set to establish guidelines and criteria to apply the law.

Thus, in the design of the Training Workshop on Personal Data, the Institute included not only dealing with the contents of both normative instruments, but was complemented with a workshop in which, interactively, the participants refined their knowledge about personal data, organization's systems, its use along other systems, among many other contents essential for the officer of the personal data to complies fully its responsibilities.

Training journeys allowed presenting a functional presentation on Electronic Registration of Personal Data Systems, an electronic tool that will give greater functionality to the development of the obligations that the law requires for Public Entities, and for InfoDF as guarantor organism.

As previously mentioned, the PDP Act was enacted on October 4th, 2008, and its main objective is to protect personal data held by the various organs of government in Mexico City.

With the publication of the Act, the InfoDF was given the task of spreading its content and the obligations implicit in it. This way the Institute led the awareness on the importance and projection involving protection work to public servants accountable and responsible for the care and treatment of personal data. This is and will be an indispensable step to achieve greater impact in protecting such information.

Similarly, establishing specific requirements to process personal data under standards that ensure its protection generates confidence on people, because they will be sure that personal data provided to public entities will be guarded, protected and used only for the reason which it was collected. Conversely, pub-

lic servants that provide personal data in their jobs are assured that their data is well-protected and used appropriately.

## Conclusions

In these first four years significant progress has been reached. We have identified areas of opportunity and set up strategies to strengthen the compliance of the right of access to public information in the Federal District. This effort was reflected by winning the first place in the national study called "Index of Access to Information in Mexico (IDAM)" elaborated by Article XIX and FUNDAR. This study analyzed different criteria (national and international) under which this right is guaranteed in the country and determined to give this award to the Federal District due to its high standards, conditions and results to protect and ensure this right.

It is still necessary to overcome the deficiencies produced by the budgetary constraints faced by the OPI's, which reduces their ability to respond to a growing number of information request. Due to complaints presented from citizens who review the agencies websites we noticed that some information is not updated in a timely manner, that the representatives from the OPI's have yet to face resistance from some of the administrative units which translates into problems to attend information requests and in many cases into omissions in the information disclosure. A greater effort is yet need to be done in order to train public servants to fulfill the requirements established by law.

We know that there is still a long way to go to strengthen access to public information and personal data protection as the cornerstone for the defense of other rights. It is essential work for its consolidation in order to ensure a social democratic state in the nation's capital, in which an informed citizenry will be capable of participating actively, defend their political and social rights, to help reduce corruption and improve their living conditions. In this way society and government will ease the transition to a more equitable and democratic society.

# The future of EU working parties' The future of privacy and the principle of privacy by design

**Ugo Pagallo and Eleonora Bassi**

## Introduction

It is not hard to understand why there are so many current publications on "the future of," say, science, law and technology, the internet, the public domain, etc. [Hugenholtz & Guibault, 2006; Zittrain, 2008; Brockman, 2009; Fernández-Barrera *et al.*, 2009; Brockman, 2010]. Whether or not you admit that we are in the midst of an "information revolution" [Bynum 2009, Horner 2010], technology is profoundly changing how we live, think, and interact. Scholars are eager to unfold the ideas that will be setting the trend in five or ten years, along with the innovations that could radically transform our entire world.

Consider the case of current legal systems and how technology affects them: while the study of this impact should not be blind to the reciprocal interaction between technology and society, we can fully grasp this transformation in three ways.

First, technology has deeply changed the approach of experts to legal information.

Secondly, technology has induced new kinds of lawsuits or has modified old forms.

Thirdly, technology has blurred traditional national boundaries as information on the internet tends to have a ubiquitous nature.

Such a threefold impact, however, has made some scholars adopt a sort of techno-deterministic stance, according to which there would be no way to shape or, at least, to influence the evolution of technology. Think about data protection and the reasons why some have announced "The End of Privacy" [Sykes, 1999], "The Death of Privacy in the 21st Century" [Jarfinkel, 2000], or "Privacy Lost" [Holtzmann, 2006]. Technology is what allows these scholars to unveil an already written future: In the digital environment, data protection would simply vanish due to the use of spyware, root-kits, profiling techniques, data mining, not to mention FBI programs like Carnivore or Magic Lantern. In everyday (or analog) life, some means like RFID, GPS, CCTV, AmI, or satellites, would lead to the same effect.

More recently, researchers pushed the issue even further by envisaging a world where we will read people's thoughts from the signals emitted by their brains: "It

will be the ultimate invasion of privacy" [Ford, 2010]. Likewise, other scholars imagine that solid-state memory will replace hard drives and we will live with pervasive computational presence: Of course, "battery size remains a barrier to progress, but this will improve, along with increased efficiency of our electronics (…). Privacy will vanish" [Garrett Lisi, 2010].

Yet, rumours of the death of privacy may have been greatly exaggerated and, what is more, these techno-deterministic approaches are liable to the criticism that John Kenneth Galbraith put forward in his own field: "The only function of economic forecasting is to make astrology look respectable."

Therefore, in dealing with "the future of privacy," this paper does not rely on prophetic powers or divinatory commitments: Rather, the aim is to draw attention to some major issues of today's data protection laws by examining the joint contribution of the EU Article 29 Data Protection Working Party (WP29) and the Working Party on Police and Justice (WPPJ). The document "The Future of Privacy" (02356/09/EN – WP168) adopted on December 1st, 2009, allows us to highlight crucial problems involving data protection today as well as to specify possible developments and changes induced by technology.

The paper is presented in three sections.

First, we examine how data protection is changing by focusing on some of the topics considered by the European WPs. Besides the need for a new legal framework in terms of globalisation and international standards, binding corporate rules and accountability, the European WPs pay special attention to technological changes and "Privacy by Design as a new principle." In a nutshell, the formula implies that data protection should be "embedded" in ICT through default settings, enabling business, public sector, as well as individuals to "take relevant security measures by themselves."

Secondly, we look at some highly debatable conclusions of EU WPs, namely, matters of jurisdiction on the internet. If we admit that cookies amount to 'equipment' pursuant to art. 4(1)c of Directive 95/46/EC, we end up in a paradox: According to WPs's opinion, if a US citizen is accessing a US web site during the 3rd ISIL-meeting in Corfu, the enforceable norms are the laws on data protection in the EU!

Thirdly, we stress some remarkable silences in the WPs's document on "The Future of Privacy." Along with DNA data and biometrics, such silences concern the EU Directive 2003/98/EC on the processing and re-use of the public sector information (PSI). This is telling because the rules adopted by the EU legislator aim to overcome some barriers limiting the re-use of PSI, while subordinating such re-use to the provisions on the protection of personal data. Once the goal is to create

or promote added-value services with macro-economic relevance – like what we find in the U.S. nowadays – we need to prevent the risk that today's information society refrains from re-use of PSI in Europe, due to the potential liability deriving from privacy protection.

Such a problem suggests that we deepen the "new principle" of privacy by design. The ubiquitous nature of the internet, in fact, does not only transcend traditional legal borders – thereby prompting EU WPs to admit that "global standards regarding data protection are becoming indispensable" – because the internet also questions the notion of the law as made up of commands enforced through physical sanctions. By allowing business, public sector, and individuals to take "relevant security measures by themselves," the new approach of "privacy by design" reformulates the enforcement of data protection as a matter of "restricted access" and "limited control" [Tavani, 2007].

## A sketch of the future

EU WPs's document on "The Future of Privacy" focuses on five main points, namely, i) the need for a new comprehensive legal framework; ii) technological changes and privacy by design as an innovative principle; iii) the empowering of data subjects; iv) the strengthening of data controllers' responsibility; v) stronger and clearer roles for Data Protection Authorities (DPAs), and their cooperation within the EU. Although the central message of the document "is that the main principles of data protection are still valid despite the new technologies and globalisation," the document stresses that we need to clarify some key rules and principles of the legal framework, such as consent and transparency, so as to introduce further principles in order to strengthen the effectiveness of the system.

The reason making this integration necessary depends on the restructuring of the EU institutions following the Lisbon Treaty that entered into force on December 1st, 2009. The former division between pillars have been replaced by a new horizontal approach to data protection and privacy pursuant to art. 16 of the Treaty on the Functioning of the European Union (TFEU).

However, there is a further reason for reshaping the current legal framework: It depends on the very evolution of the internet. According to the U.S. President's principal advisors on telecommunications and information policy – that is, both the National Telecommunications and Information Administration (NTIA), and the Assistant Secretary of Commerce for Communications and Information, Lawrence Strickling – we need an "Internet Policy 3.0 (…) to respond to all the social changes being driven by the growth of the Internet." More particularly, in the case of data protection, the issue can be summarized in the following way: "How can we enable the development of innovative new services and applications that

will make intensive use of personal information but at the same time protect users against harm and unwanted intrusion into their privacy?" [Strickling, 2010]

Hence, in order to strike a fair balance between people's privacy and, say, "the development of innovative new services and applications" like social network services or cloud computing, let us have a closer look at these five main points, according to which the EU WPs's document on "The Future of Privacy" addresses the general subject of today's data protection.

### *A comprehensive legal framework*

There are two peculiarities of EU law on data protection [Pagallo, 2008].

The first distinctive feature concerns the aim to ensure a "general and harmonized protection" of people's privacy within the 27 Member States of the Union: For instance, in the U.S., the Supreme Court has declared that "the protection of a person's general right to privacy [is] left largely to the law of the individual States" [Katz v. U.S., 389 U.S. 347, 350-51 (1967)]. In the European Union, the Court of Justice has affirmed that all Member States have the duty to implement the general standard of protection established by the European directives [C-101/01, Lindqvist case, § 96].

The second peculiarity involves the aim of the law, *i.e.*, why EU legal system aims to guarantee such a "general protection." While it is debatable whether or not a property standpoint prevails in the U.S. [Lessig, 2002; Volkman, 2003], it is pretty clear that data protection is considered as an autonomous fundamental right in Europe. In the opinion of the German Constitutional Court, both the confidentiality and integrity of information technology systems represent basic constitutional rights of the individual [BVG's Judgement from February 27th, 2008, 1 BvR 370/07; 1 BvR 595/07].

Following these premises, the EU WPs have declared in the document on "The Future of Privacy" that both key notions and main principles of the Directive 95/46/EC on data protection should be deemed the "backbone" of a more comprehensive legal network. This does not mean that some of these concepts need not be clarified as in the case of "consent" and "transparency" (see below 2.3).

Besides, it does not follow that some innovations are unnecessary: The WPs think it is crucial to enhance the level of data protection through specific regulations, in accordance with the general principles of "privacy by design" (upon which *infra* 2.2), and of accountability (2.4). Among the specific issues put forward by the document, we find national security policy, police and judicial cooperation, security breaches, privacy tools and services such as seals and audits. Further de-

tailed regulations would be necessary for a number of sectors like public health, employment, and intelligent transport systems.

However, the document admits that it would be meaningless to set up this comprehensive legal framework, without considering trends of globalisation: "Even though the individual often lives a local life, he can more and more be found on line where his data are processed globally. Globalisation therefore is linked to technology, the position of the data subject, data controller, DPAs/WP29 and law enforcement."

Accordingly, we need to take into account current technological changes in order to ensure the general protection of people's personal data through a more comprehensive legal framework. After all, the WPs recall that basic concepts of the first European directive on data protection (D-95/46/EC) developed in a world where information processing was characterized by "card index boxes, punch cards and mainframe computers."

### *Technological changes and privacy by design*

The idea of embedding data protection safeguards in ICT is not totally new. While art. 17 of D-95/46/EC lays down the obligation of data controllers to implement appropriate technical and organizational measures, recital 46 of the same European directive requires that such measures have to be taken "both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing."

In the late 1990s, the concept of "Privacy by Design" was further developed by the Ontario's Privacy Commissioner, Ann Cavoukian, to cope with the "ever-growing and systemic effects" of both ICT and large-scale networked data systems. In April 2000, a working paper on "Privacy Design Principles for an Integrated Justice System" was jointly presented by the Ontario's Privacy Commissioner and the U.S. Department of Justice [Cavoukian, 2009].

Yet, at least in Europe, the EU WPs admit that the provisions of the Directive have been insufficient and, therefore, "the new legal framework has to include a provision translating the currently punctual requirements into a broader and consistent principle of privacy by design. This principle should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT."

More specifically, the EU WPs single out some of the goals that should be reached, *e.g.*, data minimization and quality of the data, together with its controllability, transparency, confidentiality, and user friendliness of information inter-

faces. Among the examples of how the new principle can contribute to better data protection, the EU WPs recommend that biometric identifiers "should be stored in devices under control of the data subjects (i.e., smart cards) rather than in external data bases." In addition, the EU WPs suggest that making personal data anonymous both in public transportation systems and in hospitals should be considered a priority. In the first case, video surveillance must be designed in such a way that faces of individuals cannot be recognizable; in hospitals' information systems, patient names should be kept separated from data on medical treatments and health status.

Besides the proposals of the EU WPs, the idea of incorporating data protection safeguards in ICT has been discussed by scholars as, for instance, in the recent "Intelligent Privacy Management Symposium" at Stanford University, CA., on March 22nd-24th, 2010 [the program is online at http://research.it.uts.edu.au/magic/privacy2010/]. Moreover, in section 4, we further examine why the principle of privacy by design is particularly relevant when examining the implementation of the European directive on the re-use of PSI.

For the moment, it suffices to recall what the EU WPs claim in the light of the abovementioned recital 46 of the European directive on data protection, namely, that the principle of privacy by design should be applied "as early as possible." This seems indeed to be another case where prevention is better than cure.

### *Empowering the data subjects*

Individuals' rights to data protection must go hand in hand with the obligations for the entities that process personal data. Among the main individuals' rights we find open access to personal data, the ability to modify and to delete that data, and the right to refuse at any given time to have such data processed. Among the main obligations of the data controllers, there is the duty of processing personal data fairly and lawfully, by informing the individuals so as to gain their consent when required by the law. Furthermore, data controllers must protect the processing with security measures and filing processing with local public authorities pursuant to recital 25 of the Directive 95/46/EC.

In the opinion of EU WPs, however, current technological developments have profoundly impacted on this legal framework, so that changes in the behaviour and role of the data subjects require strengthening the position of the individuals. The document on "The Future of Privacy" stresses five points.

First, there is the need of improving redress mechanisms with the introduction of class actions procedures which already exist in the EU environmental law.

Secondly, transparency is a pre-requisite for individuals to give their valid consent. Along with new ways to inform data subjects in relation to behavioural advertising, a general privacy breach notification should be introduced in the new legal framework.

Thirdly, it is apparent that technological developments require a careful consideration of consent because, especially on the internet, implicit agreement does not always mean unambiguous consent. In the words of the U.S. Assistant Secretary of Commerce for Communications and Information, "more and more personal data was being collected leading to a growing unease with the 'notice & choice' model. How many of us really read those privacy policies or just click away at the 'Yes, I agree…' in order to get on with what you want to buy, read or post?" [Strickling, 2010]

Fourthly, there is a problem of harmonisation: The interpretation of the EU data protection laws is now and then inconsistent and many Member States have implemented neither the liability provision nor the possibility to claim non-economic damages set up by the Directive from 1995.

Finally, a lack of safeguards surrounds the ever-growing number of cases involving the individuals who upload their own personal data onto the internet, *e.g.*, via online social networks or cloud computing services. For instance, the creation of pre-built profiles of non-members through the aggregation of data, which is independently contributed by the users of social network services, lacks a legal basis or, perhaps worse, leads to incongruous outcomes. It is sufficient to recall what the Article 29 Data Protection Working Party denounced in its Opinion 5 from June 2009 (01189/09/EN WP 163): "Even if the SNS [social network service] had the means to contact the non-user and inform this non-user about the existence of personal data relating to him/her, a possible e-mail invitation to join the SNS in order to access these personal data would violate the prohibition laid down in Article 13.4 of the ePrivacy Directive [*i.e.*, D-2002/58/EC] on the sending of unsolicited electronic messages for direct marketing purposes."

### *Strengthening the responsibility of data controllers*

Dealing with the main obligations of data controllers (see above 2.3), the EU WPs regret that "compliance with existing legal obligations often is not properly embedded in the internal practices of organizations." The effectiveness of the provisions of D-95/46/EC thus require a number of pro-active measures: Data controllers should adopt internal policies and processes, while defining the mechanisms in order to execute them. Moreover, organizations should draft compliance reports and carry out audits and privacy impact assessments, so as to obtain third-party certifications or seals.

Yet, the document on "The Future of Privacy" warns that "Web 2.0 services and cloud computing are blurring the distinction between data controllers, processors and data subjects." In its Opinion the 1st of February 2010 on the very concepts of "controller" and "processor" (00264/10/EN WP 169), the WP29 remarks that "the concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis. Therefore, determining control may sometimes require an in-depth and lengthy investigation."

Nevertheless, many doubts persist despite such an in-depth and lengthy investigation. Consider the twelfth example of the abovementioned WP29's Opinion 5/2009 on social networks: "Social network service providers provide online communication platforms which enable individuals to publish and exchange information with other users. These service providers are data controllers, since they determine both the purposes and the means of the processing of such information."

Hence, would a SNS be responsible for damages caused by its users' uploading data?

While many legal systems, among which the U.S. federal law, provide for safe harbours or limitations on liability for the internet intermediaries in the case of unlawful users' conduct or user-generated content, the situation is far from clear in Europe [Pagallo, 2009].

On one side, an Italian Court admitted the responsibility of the internet providers when sentencing some of Google's executives in the Vividown suit for allowing a video to be posted online showing an autistic youth being abused [Tribunal of Milan, decision 1972 from February 24th, 2010]. According to the ECJ decision on March 23rd, 2010, in *Google v. Louis Vitton* (case 236/08), "in order to establish whether the liability of a referencing service provider may be limited under Article 14 of Directive 2000/31, it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores" (§ 114 of the decision). In other words, it as all about "the actual terms on which the service in the cases in the main proceedings is supplied," so that the Court of Paris should "assess whether the role thus played by Google corresponds to that described in paragraph 114 of the present judgment" (ibid., § 117).

On the other side, the aforementioned WP29's Opinion on social networks suggests how the liability of SNS should be grasped: SNS are only obliged to provide information and adequate warning to users about privacy risks when uploading

data, so that "users should be advised by SNS that pictures or information about other individuals, should only be uploaded with the individual's consent" [see also Sartor & Viola, 2010].

Therefore, at the end of the day, what do we really mean by strengthening the responsibility of data controllers? Do we want data controllers to be obliged to monitor the network in an unprecedented and perhaps unmanageable manner? Does art. 15 of the EU Directive 2000/31/EC on e-commerce rule out this duty, in 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 to actively seek facts or circumstances indicating illegal activity"?

Moreover, what about matters of jurisdiction between, say, EU and U.S.? Are today's standard international legal approaches sufficient or should we look for alternative ways in coping with global privacy issues?

In order to further clarify some of these questions, let us proceed with the analysis of "The Future of Privacy": The WPs's remarks on both the role and functions of the European authorities on data protection allow us to straighten on some of these problems.

## *The role of the authorities*

The fifth (and final) issue examined by the EU WPs's document on "The Future of Privacy" concerns the role of the Data Protection Authorities (DPAs). The subject is particularly relevant for three reasons.

First, notwithstanding the limits on which we insist below, EU DPAs' role has been altogether positive, specially when you compare it with the functioning of the U.S. Privacy and Civil Liberties Oversight Board under the Bush administration. To sum the point up with the Director of the ACLU's Technology and Liberty Program, Barry Steinhardt, "when it comes to how we handle privacy, America should be moving toward Europe – not forcing them to move toward us" (Steinhardt's statement from February 2nd, 2004, is online at http://www.aclu.org/technology-and-liberty/new-report-shows-why-americans-must-join-europeans-protect-privacy-aclu-says).

Secondly, despite this positive record, the role of DPAs can be improved. As stressed by the EU WPs's Opinion, there are still big differences regarding the position of DPAs in the twenty seven Member States of the Union, while art. 28 (1) of D-95/46/EC is unclear with regard to their true independence.

Similarly, a new legal framework should include both DPAs's power to impose financial sanctions on controllers and processors, and their role as a consulta-

tive body in future legislation on data protection. Taking into account changing contexts within the EU, changing emphasis in law enforcement and unmet challenges for data protection such as data mining, intelligent CCTVs, biometric tools, and the risk of growing inaccuracies, *e.g.*, cases of false negatives- and false positives-subjects, the thesis of the EU WPs's document is that "cooperation between DPAs in charge of ensuring lawfulness of data processing should be strengthened in all matters and integrated in the legal framework, also by envisaging stable mechanisms (…) in order to foster a harmonised approach across the EU and beyond."

Finally, the role of DPAs brings us back to matters of enforceability and jurisdiction. As mentioned above (see supra 2.1), data protection is a fundamental right under EU law, so that, in the opinion of the WPs, "the EU and its Member States should guarantee this fundamental right for everybody, in so far as they have jurisdiction. In a globalised world, this means that individuals can claim protection also if their data are processed outside the European Union."

However, the same document recalls the indispensability of global standards and the necessity of international agreements for the protection of personal data in today's context. The document on "The Future of Privacy" singles out specific forms of international and even of transnational cooperation such as the Binding Corporate Rules (BCRs), *i.e.*, international codes of conduct for multinationals in order to regulate the worldwide transfer of data.

Thus, let us clarify how there may be a problematic divergence between the harmonization of law-making within the EU and the call for international cooperation. A good example of such a divergence is the case of transnational cookies.

## Transnational cookies

Before we illustrate the EU WPs's Opinion on the legal status of cookies, that is, the file-texts put on your computer's hard disk by a web site when you are accessing it, we need to define what 'transnational' law really means. By comparing this adjective with the more frequent term of 'international' law – in all likelihood coined by Jeremy Bentham – some basic Latin helps.

On one hand, 'inter' means 'between' or 'in-between.' According to the standard Westphalian model, international law is in fact the law between sovereign nation-states and not, say, between their citizens or subjects. As stressed by Jack Goldsmith, the (traditional) idea is that "in the absence of consensual international solutions, prevailing concepts of territorial sovereignty permit a nation to regulate the local effects of extraterritorial conduct" [Goldsmith, 1998].

On the other hand, 'trans' means 'beyond' so that transnational law implies something that lays beyond nation-states and their control, *i.e.*, it is entwined with

international law but does not coincide with it. One of the first occasions when the formula was used, is Philip Jessup's characterization of transnational law as "all law which regulates actions or events that transcend national frontiers. Both public and private international law are included, as are other rules which do not wholly fit into such standard categories" [Jessup, 1956].

More than half a century later, the "other rules" of Jessup's definition of transnational law may be summed up in accordance with the multiple fields where this idea "has proven most fruitful and provocative" [Zumbansen, 2008]: Think about *lex mercatoria*, corporate governance, public international law, human rights litigation, and even transnational citizenship [Bauböck, 1994]. In this category, we should add the realm of ICT law and the cyberspace, on which the EU WPs have been focusing in several Opinions and other contributions mentioned here. Following David Post's critique of Goldsmith's traditional ideas on international law, information technology has produced "a world in which virtually all events and transactions have border-crossing effects" and, therefore, such "effects and transactions, previously at the margins of the legal system and of sufficient rarity to be cabined off into a small corner of the legal universe (…) have migrated, in cyberspace, to the core of that system" [Post, 2002].

Consequently, when examining some typical cross-border effects of cyberspace, *e.g.*, jurisdictional issues of personal data protection, what law applies? Is it the law of the sovereign national state which disciplines the local effects of extraterritorial conduct or the "other rules" of transnational law? More particularly, when an EU citizen is accessing a web site whose equipment is located outside the EU, are the EU laws on data protection enforceable?

In the next section (3.1), we examine the thesis put forward by the EU Article 29 Data Protection Working Party since its Opinion from May 30th, 2002 (5035/01/EN/Final WP 56).

Then (3.2), we illustrate some flaws in the thesis.

Finally (3.3), an alternative way to approach the issue is suggested.

## *EU laws in cyberspace*

In the aforementioned document from 2002, the WP29 declared the EU law to be applicable, when a "US web site puts a cookie on the personal computer of individuals in the EU in order to identify the PC to the web site in view of linking up that information with others." There are two reasons why:

First of all, in accordance with the thesis on the principle of sovereignty and "a nation's right to control events within its territory" [Goldsmith, 1998], the WP29 claimed that "a survey of international law suggests that States have a tendency

to use several alternative criteria for determining extensively the scope of application of national law" (see again Document 5035/01/WP56). Specifically, the criterion adopted by the WP was that 'equipment' included cookies pursuant to art. 4 (1)c of D-95/46/EC: "Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data when (…) 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 State."

Secondly, the WP29 argued that the aim is not only to extend the range of applicability of EU law but, rather, to ensure the protection of people's rights: "The objective of this provision in Article 4 paragraph 1 lit. c) of Directive 95/46/EC is that an individual should not be without protection as regards processing taking place within his country, solely because the controller is not established on Community territory. This could be simply, because the controller has, in principle, nothing to do with the Community. But it is also imaginable that controllers locate their establishment outside the EU in order to bypass the application of EU law."

(More recently, as we mention in section 2.5, the EU WPs's document on "The Future of Privacy" admits that "article 4 of the directive, determining when the directive is applicable to data processing, leaves room for different interpretation." Nevertheless, in accordance with the previous opinion from May 30th, 2002, they insist that the protection of people's fundamental rights "means that individuals can claim protection also if their data are processed outside the European Union.")

Of course, one could rebut the twofold argument of the WP29's document, by observing that, from a historical perspective, the protection of fundamental rights questions the idea of the law being based upon the principle of sovereignty. Moreover, in the case of cyberspace, we should add that "all conduct has geographically far-flung effects on people and institutions around the world" so that "there will continually be conflicts between a principle that permits sovereigns to regulate on the basis of those effects, and a principle that sovereigns can only regulate where they have the consent of the regulated" [Post, 2002].

Still, there are more pragmatic reasons for considering the EU WP's reasoning weak. They concern the legislation of every single Member State of the EU and how foreign companies could exclude EU users from their services. Let us examine more carefully some of these criticisms.

## *Pan-jurisdiction and its paradoxes*

Scholars often stress why it is wrong to hold cookies to be an 'equipment' pursuant to art. 4 (1)c of D-95/46/EC. In this context, it is enough to mention five reasons.

First, among the definitions of art. 2 of D-95/46/EC, 'equipment' is not legally defined: To consider cookies as a sort of equipment would be more a matter of political choice than of legal interpretation.

Secondly, many EU provisions apply to non-European companies doing business in Europe: This entails evident issues in the field of consumer law for instance. Many of these companies have thus trouble excluding EU users from their services, in that such companies, in order to do so, would need to establish residence and name of such users, which clearly entails potential infringements on data protection and other issues of jurisdiction: Ultimately, this leads to a vicious circle.

Thirdly, by considering cookies as an 'equipment', the principal criterion according to which EU Member States should apply the directive would not hinge on the place where the data controller is established. Rather, contrarily to the rationale of the directive, its applicability would depend on the emplacement of the data subject.

Fourthly, by applying EU data protection laws to all the websites using cookies on the internet, foreign data controllers would be compelled to simultaneously comply with the legislation of every single Member State of the EU, which raises an "impossible burden" [Kuner, 2003].

Fifthly, there is the paradox mentioned in the introduction of this paper. Once you admit that cookies constitute an 'equipment', it follows that every time a US citizen is accessing a US website during, say, a holiday in Europe, the enforceable norms would be the EU laws on data protection.

In the light of these and other possible shortcomings, are there alternative ways to deal with the drawbacks of the EU jurisdiction?

### *Feasible way outs*

In his Opinion from July 25th, 2007 (2007/C 255/01), the European Data Protection Supervisor (EDPS), Peter Hustinx, recalled the ECJ decision of the Linqvist case (see above 2.1), in order to warn how "this system, a logical and necessary consequence of the territorial limitations of the European Union, will not provide full protection to the European data subject in a networked society where physical borders lose importance (…): the information on the Internet has an ubiquitous nature, but the jurisdiction of the European legislator is not ubiquitous."

In fact, cyberspace issues, like other cases put forward by contemporary *lex mercatoria*, corporate governance, or human rights litigation, show the limits of current international approaches based upon the principle of sovereignty and the nations' right to unilaterally control events within their territories. As proposed by Peter Hustinx in the aforementioned Opinion, the challenge of protecting personal

data on the international level "will be to find practical solutions" through typical transnational measures such as "the use of binding corporate rules by multinational companies" and "international agreements on jurisdiction." Furthermore, there is the need of "promoting private enforcement of data protection principles through self-regulation and competition," while "accepted standards such as the OECD-guidelines for data protection (1980) and UN-Guidelines could be used as basis."

Quite significantly, this is also what the EU WPs have somehow proposed in "The Future of Privacy," when remarking the importance of both international agreements and codes of conduct for multinationals, together with global standards regarding data protection (see above 2.5).

Besides, global issues of data protection could be effectively analyzed through EU WPs's "idea of incorporating technological protection safeguards in information and communication technologies," *i.e.*, according to the principle of privacy by design, which "should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT" (see supra 2.2).

So, in order to further illustrate how the principle may function, let us introduce this new topic of design and the field of personal data protection: Even though the EU WPs have not examined the subject matter in their Opinion, the realm of the public sector information (PSI) helps us shed new light on "The Future of Privacy."

## The troubles with public sector information

Silence can be more telling than words. It is indeed striking that neither the document on "The Future of Privacy" nor the 2010-2011 program of the EU Working Party art. 29 mention the directive 2003/98/EC. This set of rules subordinates the processing and re-use of the public sector information (PSI) to the provisions of D-95/46/EC on the protection of personal data [see art. 1 (4) of the PSI directive in the next section].

Eventually, there are some reasons explaining this otherwise puzzling silence.

On the one hand, notwithstanding the potential of PSI [Aichholzer & Burkert, 2004; Hugenholtz & Guibault, 2006], many EU Member States have inappropriately implemented the directive. It suffices to recall that the European Commission has taken five Member States – *i.e.*, Austria, Belgium, Portugal, Spain and Luxembourg – to the European Court of Justice for failing to implement the directive and, on March 19th, 2009, the Commission filed another infringement procedure against Italy.

On the other hand, even where Member States have started to exploit the potential of both PSI and the PSI directive, most of the data present little or no reference with people's personal data. So far, we are mostly talking about the re-use of, say, geographic information, army maps, land register and meteorological data, museums and local archives metadata, etc.

However, we need no prophetic powers in order to foresee that further implementation of the PSI directive will necessarily imply a number of privacy issues. Whereas the goal of the directive is to remove some of the barriers that are limiting the re-use of PSI, it is likely that the creation of added-value services with macro-economic relevance, like American PSI provides to the U.S. today, will run into the EU provisions on data protection.

This is precisely what both the Agencias de Protección de datos in Madrid and Barcelona stressed with their "Recommendations" from 2008. By paying attention to the possible re-use and processing of such data like civil service repositories, electoral data, universities' databanks, and the like, these Agencies insist on the necessity of adopting security measures and special regimes, along with the condition for habeas data guarantees like access, rectification, erasure, and blocking.

Moreover, the aforementioned Opinion on the concepts of "controller" and "processor" that the WP29 delivered on February 16th, 2010, is an important document, not centered on PSI and, yet, very interesting for our purposes. By examining cases of multiple controllers and processors in order to allocate responsibility in the legal system, the Opinion introduces some possible scenarios of interaction between D-2003/98/EC and D-95/46/EC.

Nonetheless, both the Recommendations and the WP29's Opinion fall short in coping with the risk that today's Information Society refrains from PSI re-use because of liabilities deriving from personal data protection. In order to illustrate this, let us examine the Spanish Recommendations from Madrid and Barcelona (section 4.1).

Then, we discuss the WP29's Opinion from 2010 (see below 4.2).

Finally, we introduce the "new principle" of *PSI by design* (section 4.3).

### *Spanish recommendations*

A merit of the 2008 Spanish recommendations consists in having shed light on the relation between data protection norms and PSI re-use rules pursuant to art. 1 (4) of this latter directive, *i.e.*, D-2003/98/EC, which "leaves intact and in no way affects the level of protection of individuals with regard to the processing of

personal data under the provisions of Community and national law, and in particular [it] does not alter the obligations and rights set out in Directive 95/46/EC."

According to the Agencia in Madrid, when processing and re-using PSI data, data controllers should follow some basic principles on the treatment of personal data. As stressed by the Recomendación 2/2008 from April 25th, such data should be "indispensable" and "minimized," so that the default rule provides for making such data anonymous most of the time, erased as soon as possible and, in any event, kept no longer than six months. Besides, the Agencia envisages additional specific regulations for both electoral and administrative data, in accordance with the architecture of that comprehensive legal framework later sponsored by the EU WPs's document on "The Future of Privacy" (see above 2.1).

In its recommendation 1/2008 from April 15th, the Agencia in Barcelona points out eight general conditions for the transmission of information on the internet, namely, the legitimacy and proportionality of the information, the exactitude and updating of the information transmitted, the time limits of the transmission and the periodic review of the web content, besides duties on information, security measures and conditions for habeas data guarantees such as the data subject's right to access, rectify, erase, and block her data. While the aim is "to provide guidelines for action with regard to the transmission of information containing personal data on Internet websites," the recommendation is specifically "addressed to all bodies, entities and authorities forming part of or attached to public institutions in Catalonia, the Autonomous Government, local authorities [and] universities," including "public or private organizations that, in accordance with any contract, agreement or legal disposition, manage public services or exercise public functions."

However, one of the main side effects of current technological changes is that both "Web 2.0 services and cloud computing are blurring the distinction between data controllers, processors and data subjects" (see above 2.4). This is relevant when determining the responsibility for compliance with data protection rules, according to the functional approach proposed by the EU WP29 on February 16th, 2010 (see again supra 2.4).

What is more, such a functional approach becomes all the more appropriate, once we grasp the range of opportunities offered by PSI. Indeed, "the creation or improvement of services resulting from the data elaboration or aggregation can be encouraged by making available decentralized choices identifying innovative ways to use PSI. (…) In these terms PSI could be perceived as a platform, of which applications are still to be identified and written, just as the Internet or the Apple's iPhone" [Ricolfi, 2010].

After the 2008 Recommendations of the Spanish agencies, let us have a closer look at this new scenario.

### *Processors and controllers*

In the aforementioned Opinion on the concepts of data processor and data controller, the WP29 insists on the necessity to adopt a functional approach in order to allocate responsibility in accordance with a substantial (rather than a formal) analysis. The WP29 proposes twenty six different examples so as to clarify its view. Here it suffices to mention example 11 of the Opinion, that is, the case of e-government portals, and example 15 on platforms for managing health data.

## The case of e-government portals

The WP's example of e-government portals is particularly interesting because PSI can be re-used both "for improving public choices (e-governance)" and "for permitting citizens to take part in the public choices in a more sophisticated way (e-democracy)" [Ricolfi, 2010].

In a nutshell, the portal acts as an intermediary between citizens and the public administration units: While the portal transfers people's requests, it also deposits the public documents until they are re-used by the citizens. Besides the responsibility of each public administration unit, which remains controller of the data processed for its own purposes, can the portal be considered data controller in this case?

According to the EU WP29, it can.

Actually, the portal should be considered as a data controller because it processes data for further purposes than those for which the data was initially processed by each public administration unit. In order to facilitate e-government services, the portal collects the requests of citizens so as to transfer them to the competent public administration unit. Besides, the portal stores the public documents so as to regulate any access to them, *e.g.*, citizens' downloading of the documents.

The result is that, among other obligations, these portals ought to ensure the security of the system when transferring personal data from the user to the system of the public administration. At the macro-level, the EU WP29 claims that such a transfer is an "essential part of the set of processing operations carried out through the portal." As an intermediary between citizens and public administration units, the portal is thus held responsible for the design of the system and how the latter processes people's personal data.

## Platforms for managing health data

The second example concerns the hypothesis of a public authority which "establishes a national switch point regulating the exchange of patient data between healthcare providers."

Paradoxically, the number of data controllers involved, namely, all of the healthcare providers, may create an "unclear situation": It is not trivial to determine whom the patients have to address in order to exercise their rights, *e.g.*, make complaints, ask questions, and send requests for information, corrections or access personal data. Since "it can be argued that joint and several liability for all parties involved should be considered as a means of eliminating uncertainties," the WP suggests an autonomous responsibility for the public authority establishing the switch point.

At the end of the day, the public authority should be thought of both as a joint controller and as a point of contact for all of the patients' requests: This means that the public authority should be held responsible for the design of the platform and, therefore, indirectly, for how patients' data is used and processed.

This latter responsibility brings us back to the risk that public authorities may refrain from PSI re-use due to the cumbersome responsibilities deriving from personal data protection. It would not be the first time privacy is evoked so as to protect inertia or, even worse, to "conceal some sort of fraud" [Posner, 1983].

## *PSI by design*

A "new principle" in the phrasing of the EU WPs's document, "Privacy by Design" is the subject of a number of works mainly focusing on data protection issues involved in the design of IC technologies [Abou-Tair and Berlik, 2006; Mitre *et al.*, 2006; Lioukadis *et al.*, 2007]. As Herbert A. Simon pointed out in his seminal book on *The Sciences of Artificial*, "in substantial part, design theory is aimed at broadening the capabilities of computers to aid design, drawing upon the tools of artificial intelligence and operations research" [Simon, 1996]. While scholars increasingly stress the specific impact of design or "architecture" and "code" on legal systems [Lessig, 1999; Katyal, 2002¸2003; Zittrain, 2008], it is interesting to further understand how artificial intelligence and operations research may aid design and, in doing so, impact on the structure and evolution of legal systems [Pagallo, 2007].

A mention should be made of an ongoing project on the "Neurona Ontology" developed by Pompeu Casanovas and his research team in Barcelona [Casellas *et al.*, forthcoming]. The overall idea is to assume "ontologies" as the key form to

implement new technological advances in the fields of both managing personal data and providing organizations and citizens "with better guarantees of proper access, storage, management and sharing of files." The explicit goal of the project is to help company officers and citizens "who may have little or no legal knowledge whatsoever."

Legal ontologies aim to represent knowledge through the modelling of concepts traditionally employed by lawyers, by formalizing norms, rights, or duties, in criminal law, administrative law, etc., in such a way that even a machine can comprehend and process this very information. We can further distinguish between the ontology containing all the relevant concepts of the problem domain through the use of taxonomies, and the ontology including rules and constraints that belong to a given problem domain [Breuker *et al.*, 2008]. An expert system should allow us to re-use PSI data in compliance with regulatory frameworks in data protection, as with e-government portals or healthcare switch points, via the conceptualization of classes, relations, properties, and instances of the problem domain.

Still, it could be argued that data protection regulations do not only include "top normative concepts" like validity, obligation, prohibition, and the like. These rules present highly context-dependent normative concepts such as notions of personal data, security measures, or data controllers. These notions raise a number of relevant questions when reducing the informational complexity of a legal system in which concepts and relations are subject to evolution [Pagallo, 2007, 2010]. After all, we have analyzed some hermeneutical issues on data protection law, *e.g.*, matters of jurisdiction and sound definitions of equipment, which can be hardly reduced to an automation process. In the phrasing of Karen Yeung, "a rich body of scholarship concerning the theory and practice of 'traditional' rule-based regulation bears witness to the impossibility of designing regulatory standards in the form of legal rules that will hit their target with perfect accuracy" [Yeung, 2007].

Such technical difficulties in achieving the "perfect enforcement" of the law [Zittrain, 2007], illustrate why several projects concerning legal ontologies have adopted a bottom-up rather than a top-down approach, that is, "starting from smaller parts and sub-solutions to end up with global" answers [Casellas *et al.*, forthcoming]. While splitting the work into several tasks and assigning each to a working team, the evaluation phase consists not only in testing the internal consistency of the project but, according to Simon's "generator test-cycle," it involves the decomposition of the complete design into functional components. By generating alternatives and testing them against a set of requirements and constraints, "the test guarantees that important indirect consequences will be noticed and weighed. Alterna-

tive decompositions correspond to different ways of dividing the responsibilities for the final design between generators and tests" [Simon, 1996].

This ability to tackle our own ignorance helps us striking a balance between the know-how of legal ontologies and its limits. In a nutshell, the aim concerns privacy and PSI-reuse 'by' design, not 'as' design, *i.e.*, as if the goal were a sort of perfect self-enforcement technology which "collapses the public understanding of law with its application eliminating a useful interface between the law's terms and its application" [Zittrain, 2007]. What at stake, indeed, is the integration of compliance with regulatory frameworks through design policies, so that "privacy assurance must ideally become an organization's default mode of operation" [Cavoukian, 2009]. From the unfeasibility of automatizing all the mechanisms of data protection it does not follow the impossibility to restrict the discretion of company officers or public bureaucrats, while enhancing people's rights and encouraging behavioural change [Casanovas, 2009].

## Conclusions

Along with "the future of" science, law and technology, the internet, the public domain, etc, scholars have often coped with "The Future of Privacy": For instance, this is precisely the subject matter of the last chapter of a comparative study on data protection published some years ago [Pagallo, 2008].

On that occasion, the forecast was summed up with the formula of "civic emergence" and the new ways in which we should grasp the interaction between private corporations and the public sector in the field of privacy law.

On one side, in spite of the threats to privacy created by the G. W. Bush's administration and its "war on terror," *e.g.*, the provisions of The Patriot Act, a reason of major concern involved databanks owned by private corporations. This was the case of the Canadian Internet Policy and Public Interest Clinic (CIPPIC)'s complaint against Facebook in May 2008, besides Facebook's own "terms-of-service"-crisis from February 2009 & May 2010, and the letter sent to Google's chief executive officer, Eric Schmidt, on April 19th, 2010. In the letter, the Privacy Commissioner of Canada, Jennifer Stoddart, and the heads of the data protection authorities of France, Germany, Israel, Italy, Ireland, Netherlands, New Zealand, Spain, and the United Kingdom, expressed their fears about privacy issues related to the new services of Google Buzz: "We therefore call on you, like all organizations entrusted with people's personal information, to incorporate fundamental privacy principles directly into the design of new online services."

On the other side, notwithstanding PET techniques, *e.g.*, encryption, it is all about the risks behind the use of commercial data, processed by private companies, in

the name of alleged public interests. Starting with the Hadopi law passed by the French Parliament on October 22nd, 2009, it suffices to recall the "three strikes"-doctrine, that is, the law according to which internet users ought to be logged off after three notices of copyright infringement. The risk is that "feeling of permanent control" stressed by the German constitutional court in its judgment on data retention from March 2nd, 2010 [1 BvR 256/08].

Hence, some years after that 2008 forecast, how are the stars aligning today?

We propose to single out three aspects of the question.

First, it is likely we need to empower the data subjects over the next years as we define the responsibility of data controllers and strengthen the role of the public authorities in data protection: Will it prevail the open approach of EU WP29's Opinions or the more prudent ECJ jurisprudence?

Secondly, we need to mention some of the open issues that the WPs did not address in their document, *e.g.*, the new frontiers of biometrics and the relation between norms of PSI re-use and data protection provisions. It should be expected that also these subjects will contribute to work out that comprehensive legal framework required by the same European authorities.

Thirdly, we have matters of jurisdiction which the EU WPs have been debating over the last decade and that, nevertheless, are still far from finding a common, worldwide solution. Significantly, in the document on "The Future of Privacy," we are reminded that "the WP29 is writing an opinion on the concept of applicable law. The WP29 envisages advising the European Commission on this topic in the course of the upcoming year."

Yet, a final topic deserves our attention, namely, the "new principle" of privacy by design. By embedding data protection safeguards in IC technologies, the principle may represent a turning point in how we tackle most of the challenges mentioned above. Privacy by design could indeed help us strengthen people's habeas data and allow us to prevent the risk of hampering economic growth due to alleged privacy reasons. Moreover, privacy by design can represent an effective way to solve some of the extra-territorial legal effects and jurisdictional issues created by digital technology, in that privacy assurance can become a default mode of operation both for private companies and public institutions.

So, here comes our last conjecture: If it is not guaranteed that privacy by design will offer the one-size-fits-all solution to the problems we will be concerned with in the realm of data protection, privacy by design will be the key to understand how we have coped with today's privacy issues. It is not only a matter of technology, after all.

## References

Abou-Tair, D. and Berlik, S. (2006), An ontology-based approach for managing and maintaining privacy in information systems, Lectures notes in computer science, Springer, 4275: 983-994

Aichholzer, G. and Burkert, H. (2004), Public sector information in the digital age. Between markets, public management and citizen's right, Elgar Publishing

Bauböck, R. (1994), Transnational citizenship: membership and rights in international migration, Elgar Publishing

Breuker, J., Casanovas, P., Klein, M.C.A., Francesconi E. (eds.) (2008), Law, ontologies and the semantic web: channelling the legal information flood, IOS Press

Brockman, M. (ed.) (2009), What's next? Dispatches on the future of science, Vintage

Brockman, M. (ed.) (2010), This will change everything. Ideas that will shape the world, Harper

Bynum, T. W. (2009), Philosophy and the information revolution, CEPE 2009: Eighth International Conference of Computer Ethics: Philosophical Enquiry, 26-28 June 2009, Ionian Academy Corfu, Greece

Casanovas, P. (2009), The future of law: relational justice and next generation of web service. In Fernandez-Barrera *et al.* (Eds.) (2009), Law and technology: looking into the future, European Press Academic Publishing, 137-156

Casellas, N., Torralba, S., Nieto, J.-E., Meroño, A., Roig, A., Reyes, M. and Casanovas, P. (forthcoming), The neurona ontology: a data protection compliance ontology

Cavoukian, A. (2009), Privacy by design, IPC Publications

Fernandez-Barrera, M., Nuno Gomes de Andrade, N, de Filippi, P., Viola de Azevedo Cunha, M., Sartor, G., and Casanovas, P. (eds.) (2009), Law and technology: looking into the future, European Press Academic Publishing

Ford, K. W. (2010), Reading minds, in Brockman, M. (ed.), This will change everything, Harper, 141-142

Garrett Lisi, A. (2010), Changes in the changers, in Brockman, M. (ed.), This will change everything, Harper, 270-273

Goldsmith, J. (1998), Against cyberanarchy, University of Chicago Law Review, 65: 1199-1250

Holtzman, D. H. (2006), Privacy lost. How technology is endangering your privacy, Jossey-Bass

Horner, D. S. (2010), Metaphors in orbit: revolution, logical malleability, generativity and the future of the internet, ETHICOMP 2010: The "backwards, forwards and sideways" changes of ICT, edited by M. Arias-Oliva, T. W. Bynum, S. Rogerson e T. Torres-Corona, Universitat Rovira I Virgili, Tarragona, Spain, 301-308

Hugenholtz, B. and Guibaault, L. (eds.) (2006), The future of the public domain. Identifying the commons in information law, Kluwer

Jarfinkel, S. (2000), Database nation. The death of privacy in the 21st century, O'Reilly

Jessup, P. C. (1956), Transnational law, Yale University Press

Katyal, N. (2002), Architecture as crime control, Yale Law Journal, 111: 1039-1139

Katyal, N. (2003), Digital architecture as crime control, Yale Law Journal, 112: 101-129

Kuner, Ch. (2003), European data privacy law and online business, Oxford University Press

Lioukadis, G., Lioudakisa, G., Koutsoloukasa, E., Tselikasa, N., Kapellakia, S., Prezerakosa, G., Kaklamania, D. and Venierisa, I. (2007), A middleware architecture for privacy protection, The International Journal of Computer and Telecommunications Networking, 51(16): 4679-4696

Lessig., L. (1999), Code and other laws of cyberspace, Basic Books

Lessig, L. (2002), Privacy as property, Social Research, 69: 247-269

Mitre, H., González-Tablas, A., Ramos, B., and Ribagorda, A. (2006), A legal ontology to support privacy preservation in location-based services, Lecture notes in computer science, Springer, 4278: 1755-1764

Pagallo, U. (2007), "Small world" paradigm and empirical research in legal ontologies: a topological approach, The multilanguage complexity of European law: methodologies in comparison, edited by G. Ajani, G. Peruginelli, G. Sartor, D. Tiscornia European Press Academic Publishing, 195-210

Pagallo, U. (2008), La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto, Giuffrè

Pagallo, U. (2009), Sul principio di responsabilità giuridica in rete, Il diritto dell'informazione e dell'informatica, XXV(4-5): 705-734

Pagallo, U. (2010), As law goes by: topology, ontology, evolution. AICOL 2009, edited by P. Casanovas, U. Pagallo, G. Sartor, G. Ajani, Springer

Posner, R. A. (1983), Privacy and related interests, The Economics of justice, Harvard University Press, 299-347

Post, D. G. (2002), Against "against cyberanarchy", Berkeley Technological Law Journal, 17: 1365-1383

Ricolfi, M. (2010), Public sector information: a general overview, Extracting value from PSI: legal framework and regional policies, EVPSI meeting at the University of Turin, Italy, on March 26th

Sartor, G., Viola de Azevedo Cunha, M. (2010), The Italian google-case: privacy, freedom of speech and responsibility of providers for user-generated contents (May 11, 2010). Available at SSRN: http://ssrn.com/abstract=1604411

Simon, H. A. (1996), The sciences of the artificial, The MIT Press

Strickling, L. E. (2010), The internet: evolving responsibility for preserving a first amendment miracle, The Media Institute, February 24th, 2010

Sykes, C. (1999), The end of privacy. The attack on personal rights at home, at work, on-line, and in court, St. Martin's Griffin

Tavani, H. T. (2007), Philosophical theories of privacy: implications for an adequate online privacy policy, Metaphilosophy, 38(1): 1-22

Volkman, R. (2003), Privacy as life, liberty, property, Ethics and Information Technology, 5(4): 199-210

Yeung, K. (2007), Towards an understanding of regulation by design, Regulating technologies: legal futures, regulatory frames and technological fixes, edited by R. Brownsword, K. Yeung, Hart Publishing, 79-108

Zittrain, J. (2007), Perfect enforcement on tomorrow's internet, Regulating technologies: legal futures, regulatory frames and technological fixes, edited by R. Brownsword, K. Yeung, Hart Publishing, 125-156

Zittrain, J. (2008), The future of the internet and how to stop it, Yale University Press

Zumbansen, P. (2006), Transnational law, Encyclopedia of Comparative Law, Elgar, 738-754

# Privacy in the nook of Facebook

**Marinos Papadopoulos &**
**Alexandra Kaponi**

Information on the private sphere of one's life does not have a fixed and undisputed meaning in law, but rather is contextually defined by the social environment of one's life perceptions, mentations, customs of a certain social environmental context, which might be in constant flux. There are no areas of life not governed by context-specific norms of information flow and privacy is not an exception to this rule. People move into and out of a plurality of distinct contexts every day with a reasonable expectation for respect of their privacy, at least in Europe.[1] As we move between spheres of daily life, we have to alter our behaviors to correspond with the norms of those spheres, i.e. to adjust our behaviour to those spheres of daily life. Usually however we do not deprive ourselves willingly from the right to privacy despite the fact which we easily acknowledge hastily, that there will always be risks in information-sharing in the sense that information appropriately shared in one context becomes inappropriately shared in a context under different norms. Information is always tagged, as it were, with the context in which it is revealed, though in the E.U. legal framework, compared to the U.S. law,[2] there is more certainty about what information constitutes the core of privacy, personal and sensitive data and what the requirements are for legal use of it irrespective of the context that this information is used. Still, there is no such thing as context-free information; the protection of privacy makes sense both in public and in private spaces, and the meanings of privacy, public and private spaces are subject to different norms and contexts which are (re)shaped in society constantly.[3] For most of the people with no legal background, privacy and information-sharing related to it can probably better be understood in relation to the context in which information is shared.

In this work, we're approaching the context of Facebook as a social networking site with the aim to understand the level of privacy and data protection related to it. This approach is affected by the sensitivity and regulation for data protection in effect in the E.U.,[4] though we're aware of the fact that Facebook Inc., is not a legal entity based in the jurisdiction of any E.U.-member country,[5] but rather subjects to the U.S. law; yet, it may also subject to the E.U. data protection law in accordance with the legal opinion of the Article 29 Data Protection Working Party.[6] This should not drive us into the conclusion that Facebook Inc. could challenge of

operate in consideration only of the U.S. law for data protection and privacy, but rather it should consider and organize its Facebook Platform and Applications with the aim to abide by E.U. data protection regulation.[7] Facebook represents a novel phenomenon to (risk of) data protection and privacy[8] online that considers all companies of the breed of social networking sites, probably because of the fact that Facebook is the most widely known and used[9] among them.[10]

In order to define social networking sites, we consider boyd[11] and Ellison's definition of them as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.[12] The defining characteristics of a social networking site are (a) tools for posting personal data[13] into a person's 'profile' and user-created content linked to a person's interests and personal life; (b) tools for personalised, socially-focused interactions, based around the profile (e.g. recommendations, discussion, blogging, organisation of offline social events, reports of events) (c) tools for defining social relationships which determine who has access to data available on social networking sites and who can communicate with whom and how.[14]

## Research findings and studies on Facebook users

Almost all of the evidence suggests that Facebook users primarily use the social networking site to solidify and develop their offline social relationships, rather than to make new relationships online.[15] Young people primarily use online technologies to talk with people they already know.[16] Facebook claims to have an age restriction for young people under 13 years old,[17] but this age restriction and website mechanism for age verification seems to be relatively effective. For an underage user it is quite easy to cheat the age-verification mechanism by making a false statement.[18] Website safeguards, which include content advisories, age verification, or credit card verification, were found to be reasonably effective at decreasing the amount of personal information provided by children 10-12 and 13-14, but not prohibitive for participation in the Facebook Platform and Applications, which means that children 10-14 years old were able to log onto the system by making false statements regarding their age; for 15-17 year olds, safeguards created a "boomerang effect" where teens reacted negatively, attempted to circumvent the safeguards, and ultimately tended to provide more personal information than when safeguards were absent.[19]

Although users' practice to upload their information online in social networking sites is perceived to be a risk for harassment, solicitation, flaming,[20] denigration,[21] impersonation,[22] outing,[23] trickery,[24] exclusion,[25] stalking,[26] and threatening by

revealing personal information,[27] people, especially young social networking sites users tend to flirt, gossip, build relationships and hang out with peers at social networking places online.[28] The more young people use the Internet to talk to their friends and engage in playful, social behaviour, the more likely that young people is to reveal personal information and the less likely to engage in privacy-protective behaviours.[29] Moreover, research indicates that Facebook users rarely change their default privacy settings, leading to the conclusion that users are "quite oblivious, unconcerned, or just pragmatic about their personal privacy."[30] Studies show that young people conceptualize the Internet as a private space where they can share secrets and talk to their friends, behaviour that intrinsically requires the sharing of personal information.[31]

This behaviour causes privacy worries which are centred on the risks of "public living" through social networking sites such as Facebook.[32] Constant publicity of Facebook users' data tends to cause them to modify their desires and behaviors accordingly so as to cope with the fact of being public and of having all of their data that is inferred onto the system being publicly available all the time.[33] The logic is: if everything in life is an image, then images become real for us, so we tend to view ourselves in terms of the images we present, and tend to take pleasure in constructing the images of ourselves.[34] In addition, the perceived social benefits of online information-sharing seem to be perceived as outweighing any potential privacy risks.[35] The idea of being publicly and constantly available the constructed images of Facebook users on its platform at some point is in good terms with the idea of being under incessant surveillance—at least by the people who the users recognize as their friends—which causes people to stop hiding, and the panoptic principle is felt as neither a threat nor punishment, but, rather, as amusement, liberation and pleasure.[36] Information disclosure through Facebook and online popularity are interrelated and are inextricably linked. Disclosure thereby becomes an aspect of identity construction, and that construction is linked with popularity: the people who are most popular are those whose identity construction is most actively participated in by others.[37] As a result, the risks of limiting access to personal information become greater than the risks of disclosure, because when limiting access, the Facebook user also limits the potential for identity construction and thus potentially reduces his or her popularity through the Facebook Platform and Applications.[38]

## Digital dossiers, data brokering of Facebook users' personal and sensitive data, and other threats to privacy

For many people the very distinction between "public" and "private" is problematic.[39] They tend to view privacy in more nuanced ways, conceptualizing Facebook spaces as "semi-public" or "semi-private" depending on the angle they look it from or making

distinctions between different groups of "friends."[40] The urge to post as much private information on Facebook as possible with the aim to construct images of them[41] that are being constantly public is much closer to the need of Facebook users to seek publicity[42] rather than the need to protect their private information in a public forum.[43] Commercial data brokers like ChoicePoint[44] have leveraged on this need and made a (huge) profit by piecing together people's personal data to form individual profiles or "digital dossiers"[45] of people such as Facebook users who tend to put online as much personal data and information as possible.[46] Personal information is a commodity that is bought and sold by data-mining companies, marketing firms, and credit reporting agencies, and is especially valuable when coming from young people, whose consumption is a multi-billion dollar industry.[47]

The "digital dossiers" threat is not the only one, of course. There are others, too, which could result into lucrative data-mining and aggregation to the detriment of Facebook users' privacy and personal data protection.[48] ENISA has been looking at them carefully trying to shed light upon the phenomenon of social networking sites seen from the angle of information risk. Among these threats, ENISA includes the use of face recognition technologies,[49] Content-based Image Retrieval (CBIR) technologies,[50] linkability from image data,[51] difficulty to complete account deletion, SNS spamming,[52] Cross Site Scripting (XSS) viruses and worms,[53] SNS aggregators,[54] SNS phishing, profile-squatting and reputation slander through identity theft, stalking,[55] bullying,[56] and corporate espionage. In the online forum of Facebook Platform and Applications, users, unaware of the existence of data brokers or data miners that gain from personal data exploitation and trade, have come to present themselves accordingly more in consideration of taking advantage of Facebook's enhanced and inevitable publicity rather than with the aim to protect the privacy of private information which is willingly posted onto a public forum. This behaviour has been the cause for increasing use and dissemination of personal information which could set data subjects increasingly powerless and vulnerable due to lack of control of their own personal information, images and reputation.[57]

## Persistence, Searchability, Replicability, and Invisible audience

Information posted to the Internet is potentially visible by all. For most people, such universal broadcast of information has no parallel offline.[58] In other words, offline personal information is seldom communicated to a context anywhere near as broad as the entire Internet. Information flows on social networking sites such as Facebook are mediated not just by the global nature of Internet communication, but by the ways that those sites and their users interpret the meaning of online friendship and the social norms that go with it.[59] Boyd argues that social networking sites are complicating the way in which people interact because they have four properties usually not present in face-to-face public life:[60] *Persistence*:

unlike the ephemeral quality of speech in unmediated publics, networked communications are recorded for posterity. This enables asynchronous communication but it also extends the period of existence of any speech act. *Searchability*: because expressions are recorded and identity is established through text, search and discovery tools help people find like minds. *Replicability*: hearsay can be deflected as misinterpretation, but networked public expressions can be copied from one place to another verbatim such that there is no way to distinguish the "original" from the "copy." *Invisible audiences*: while we can visually detect most people who can overhear our speech in unmediated spaces, it is virtually impossible to ascertain all those who might run across our expressions in networked publics.

Also, according to Yochai Benkler, in the online context two general phenomena can be observed. First, "we see a thickening of preexisting relations with friends, family, and neighbors, particularly with those who were not easily reachable in the pre-Internet-mediated environment."[61] Second, "we are beginning to see the emergence of greater scope for limited purpose, loose relationships" as for example those surrounding topic-specific blogs.[62] Both these two phenomena exist in the Facebook environment. While in offline life privacy related to the cultivation of thick or loose relationships is a matter of face-to-face interactions and ad hoc decision making, in the environment of Facebook privacy can hardly become a matter to cope with on a case-by-case basis, but rather is merely an issue that is left to manage through the system's available privacy settings and mechanisms. Although Facebook theoretically has a highly granular set of privacy settings, users do not appear to be taking advantage of them. Research indicates that the majority of Facebook users do not understand or even read the privacy statements.[63] Or that even those who read and understand them, do not refrain from posting their personal data and information online. Acknowledgment of privacy statements and settings does not affect information provision, suggesting that ignorance of privacy statements and settings is not wholly responsible for the reluctance of Facebook users to restrict access to their profiles.[64] It is beyond doubt, though, that when the privacy statements and settings are byzantine, difficult to find, and hard to understand, then this is a main reason for the existence of users' inability to form or effectuate their privacy preferences.[65] In addition, Facebook's structure as a system which encourages a binarization of social relations into "friend" and "not friend," flattens out all of the nuances of face-to-face interactions and all the options regarding privacy protection that is judged ad hoc in offline life.[66] Thus, even if assumed that Facebook privacy statements and settings had not been byzantine, even if Facebook users had not had any difficulty in understanding and using them, their privacy options would have been quite relative in effect simply because their privacy status would subject to their friends' privacy options, as well. And a Facebook user can never command what his/her

Facebook 'friends' will opt to regarding their privacy issues as well as how the 'friends' will behave online regarding privacy protection.

Members of the Facebook community can create their own personal profile–complete with a profile photo and public photo albums, videos, and notes. They can also designate "friends," who are other Facebook users, and join virtual "Groups" that are focused around common themes and interests. Members can also choose which parts of their profile they would like to make visible to other members. Facebook also contains a "news feed," which is located on a user's Facebook homepage immediately after they log into the site. This personal news feed functions much like a typical news feed does. The basic difference is that the "news" contained in the Facebook news feed consists of profile updates made by a user's friends. Typical news stories include updates to relationship status, changes to information that members list about themselves on their profiles, and new photos that members have posted to their albums.

Facebook, that was set up by 2004, was initially only available to users who had a valid email address from a handful of colleges and universities. The site essentially served as an online, extended version of paper "facebooks" that are distributed at many college campuses to incoming freshmen. When it started, Facebook was a private space for communication with a group of a user's choice. By that time, a news feed on a user's friend could be seen only by said user. Soon, it transformed into a platform where much of a user's information is public by default, thus a news feed could be seen by any Facebook user if the content posted online was set to 'Everyone' privacy settings. In 2006, Facebook was opened to all members of the general public. Today, it has become a platform where a user has no choice but to make certain information public—'Everyone' information—and this public information may be shared by Facebook with its partner websites and used to target ads. Today, the only membership requirements are a valid email address and formal agreement to the website's Terms of Use and Privacy Policy.[67] Facebook can now gather unprecedented amounts of personal information on its users. While information disclosed is ostensibly used by Facebook to customise and personalise its services, it can also be used for targeting (e.g. advertising), discrimination (e.g. price discrimination) or the transfer of data to third parties through resale.

## Facebook Applications

In May 2007, Facebook introduced their application platform, allowing third party developers to create added functionality that links to a user's profile. These applications enhance the social experience on Facebook by allowing users to add additional content to their profiles, play games with their friends, share photos

and other media, and much more. The main three features that Facebook added to its social networking system involving partnerships with third parties were Public Search, Social Ads, and Beacon. Theses applications have been extremely successful. Facebook reports that 70% of users interact with an application each month, with over fifty thousand applications available.[68] In order to complement a user's profile, Facebook allows applications to access most of the user's profile information, except for contact information. More disturbing, however, is that these applications are also allowed to access the same information for all of a user's friends! While this allows applications to incorporate information about a user's social spheres into their functionality, few need access to such a wide variety of information to do so.

The privacy problems with such applications are easy enough to see.[69] If I join a fitness club, I expect to tell them my name and address, as well as some information about my fitness level and maybe even my doctor's name or my birthday. I do not expect to share which books and movies I like, where I went to school and where I work, and what my religious and political affiliations are or what is my sexual orientation by answering any kind of direct or indirect questions upon it. And my friends have every reason to expect that I will not share the parallel information about them with the fitness club.[70] This information sharing is largely invisible, despite the fact that Facebook self-describes its nature of operations as a mechanism that is about sharing information with others either friends or other members in the Facebook community.[71] Users are alerted with a simple message each time they install an application that both their own and their friends' information will be shared. However, this message is not very descriptive, and is easy to ignore as users are more focused on the task of using the application than on their privacy. Many users simply 'click through' these privacy notices, ignoring the one important piece of information that alerts them about giving away their information and the information of their friends to third parties.

## Facebook's incremental transformation

Facebook's incremental transformation regarding its privacy policy is indicative of the company's profitable manoeuvres in association with its advertising and business partners leveraging on the valuable personal data and information of its users.[72] Facebook originally earned its core base of users by offering them simple and powerful controls over their personal information. As Facebook grew larger and became more important, slowly but surely leveraged more and more on its users' information and personal data with the aim to profit from business partnering and advertising in exchange for sacrificing of privacy and data protection and for limiting Facebook users' options to control their own information.[73] EFF's presentation of Facebook's Privacy Policy timeline indicates gradual with-

drawing from strict data protection and privacy of personal information submitted to the system by its users.[74]

Facebook Privacy Policy circa 2005: "No personal information that you submit to Thefacebook will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings."

Facebook Privacy Policy circa 2006: "We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your school, your specified local area, and other reasonable community limitations that we tell you about."

Facebook Privacy Policy circa 2007: "Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings."

Facebook Privacy Policy circa November 2009: "Facebook is designed to make it easy for you to share your information with anyone you want. You decide how much information you feel comfortable sharing on Facebook and you control how it is distributed through your privacy settings. You should review the default privacy settings and change them if necessary to reflect your preferences. You should also consider your settings whenever you share information. … Information set to "everyone" is publicly available information, may be accessed by everyone on the Internet (including people not logged into Facebook), is subject to indexing by third party search engines, may be associated with you outside of Facebook (such as when you visit other sites on the internet), and may be imported and exported by us and others without privacy limitations. The default privacy setting for certain types of information you post on Facebook is set to "everyone." You can review and change the default settings in your privacy settings."

Facebook Privacy Policy circa December 2009: "Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings. You can, however, limit the ability of others to find this information through search using your search privacy settings."

Current Facebook Privacy Policy, as of April 2010: "When you connect with an application or website it will have access to General Information about you. The term General Information includes your and your friends' names, profile pictures,

gender, user IDs, connections, and any content shared using the Everyone privacy setting. ... The default privacy setting for certain types of information you post on Facebook is set to "everyone." ... Because it takes two to connect, your privacy settings only control who can see the connection on your profile page. If you are uncomfortable with the connection being publicly available, you should consider removing (or not making) the connection."

## Criticism by the E.U. Article 29 Data Protection Party

Facebook's withdrawal from strict data protection and privacy policy was severely criticised by E.U. data protection Authorities such as the Article 29 Data Protection Working Party which considers unacceptable the fact that the company fundamentally and incrementally changed the default settings on its social-networking platform to the detriment of a user's privacy and emphasises the need for a default setting in Facebook Privacy Policy in which access to the profile information and information about the connections of a user is limited to self-selected contacts. The Article 29 Data Protection Working Party considers that any further access to Facebook users' personal data and information, such as by search engines, should be an explicit choice of the user; additionally any use of personal data of other individuals contained in a user's profile in Facebook Platform for commercial purposes should be subject to the prior free and unambiguous consent of the data subjects as said consent is defined in E.U. data protection legislation.[75]

## The Fourth Amendment protection and the Third Party doctrine

A significant legal consequence of the voluntary sharing of people's information through Facebook and other social networking applications is that information "knowingly exposed to the public" is not entitled to privacy protection through the application of the Fourth Amendment protection in the U.S. law.[76] Which means that Facebook Inc. based in the U.S. and subject to the U.S. law primarily is not bound by the restrictions regarding privacy protection for the users of Facebook Platform and/or Facebook Applications. Where information is voluntarily shared with another party, it may be legally obtained by any third party even any Governmental agency and without a warrant.[77] Therefore, people should have no reasonable expectation of privacy in data they give to third parties such as Facebook Inc., and/or other entities through Facebook Platform and/or Facebook Applications. This standard applies equally to information truly open to the public as well as information voluntarily shared with a third party within the context of a confidential relationship, such as a business.[78] When a person reveals private information to a third party such as Facebook Inc., that individual "assumes the risk" that the third party may reveal the information to authorities

(the "third-party doctrine").[79] If the third party willingly reveals that information to the authorities, the Government and any government agency do not violate the Fourth Amendment by using it.[80] And it is doubtful whether any legal protection against them regarding said data-mining practice for investigative, surveillance or any other purposes through social networking sites can be sought, even if it's based on the Freedom of Information Act (FOIA)[81] of the U.S.[82] Not only this is true and sustainable, but also the fact that Facebook (as well as any other social network site) can be subpoenaed by a U.S. government agency[83] with the aim to provide it a Facebook user's account information and any other personal data submitted to the Facebook Platform and/or Applications by the user or any third party, even if that account is locked based on privacy settings.[84] Moreover, it should be noted that it's not only Government and government agencies such as law enforcement agencies (e.g. F.B.I.) that are not bound by the Fourth Amendment protection regarding the use of information found and retrieved through Facebook Platform and/or Applications. Employers,[85] school districts, insurance companies, direct marketing companies and corporations can and do use freely social network sites in order to collect information about prospective hires, potential law-breakers, criminal acts, students, risky behaviours, and consumer behaviour.[86]

## Trust in Privacy by Design v. Publicity by Design

In consideration of the application of the "third-party doctrine" of U.S. law in the case of Facebook Privacy Policy, it is certain that Facebook's evolving privacy policy is architecture for publicity rather than privacy. If this is a given, then Facebook's evolution seems to be in direct confrontation with the conceived need for promotion of trust in the Information Society by fostering data protection and privacy in the European market. Contrary to what is the situation in the U.S. wherein Facebook Inc. is based, in the European market individuals are at the core of the new environment of ICT and Information Society online, and an individual's privacy is protected even when personal data is submitted to any Governmental organization or any organization within the Public Sector.[87] In Europe individuals must be able to rely on ICT's ability to keep their information secure and control its use, as well as be confident that their privacy and data protection rights will be honoured in the digital space. Respect of those rights is essential in order to generate consumer trust. And such trust is crucial if citizens are to embrace new services.[88] A lack of trust in the online environment is seriously hampering the development of Europe's online economy. Among people who did not order any products or services online in 2009 and among the top reasons about it were privacy concerns, and trust concerns.[89] This envisaged trust which is of crucial importance in the E.U. online environment must satisfy the need to integrate, at practical level, data protection and privacy from the very inception

of new information and communication technologies which is referred to as the principle of "Privacy by Design."[90] The right to privacy and to the protection of personal data are fundamental rights in the E.U. which must be also online effectively enforced using the widest range of means: from the wide application of the principle of "Privacy by Design" in the relevant ICT technologies, to dissuasive sanctions wherever necessary. The E.U.'s revised legal framework for electronic communications clarifies the responsibilities of network operators and service providers, including their obligation to notify breaches of personal data security. The recently launched review of the general data protection legal framework will include a possible extension of the obligation to notify data security breaches.[91] Yet, despite this European will to reinforce the "Privacy by Design" principle in the E.U. market for the sake of trust in the ICTs and Information Society, Facebook's current Privacy Policy seems to favour the opposite, i.e. unprecedented, unrestrained, and unexceptional "Publicity by Design" rather than "Privacy by Design," thus seems to be out of context with the legal framework for data protection and privacy in the E.U.[92]

## Criticism by the E.U. Data Protection Supervisor

For this reason, the European Data Protection Supervisor has identified social networking sites such as Facebook—among other Internet applications such as RFID technology—that deserve careful consideration by the European Commission regarding data protection and privacy. Facebook as a social networking service is considered data controller insofar as it provides the means for the processing of user data and provides all the basic services related to user management.[93] In legal terms this means that Facebook users and Facebook Inc., share joint responsibility for the processing of personal data as "data controllers" within the meaning of Article 2(d) of the Date Protection Directive, albeit to different degrees and with different sets of obligations.[94] In the opinion of the E.U. Data Protection Supervisor, Facebook users by processing their personal information and that of others, they fall under the provisions of the E.U. legislation on data protection that requires, among other things, obtaining the informed consent[95] of those whose information is uploaded and granting those concerned with the right of rectification, object, etc. Similarly, Facebook as a social networking service must, among other things, implement appropriate technical and organisational measures to prevent unauthorised processing, taking into account the risks[96] represented by the processing and the nature of the data. This in turn means that Facebook as well as other social networking sites should ensure privacy-friendly default settings, including settings that restrict profile access to the user's own, self-selected contacts. Settings should also require user's affirmative consent before any profile becomes accessible to other third parties, and restricted access

profiles should not be discoverable by internal search engines.[97] However, Facebook preselects default settings based on opt-outs, thus facilitating the disclosure of personal information by default. Its current Privacy Policy enables profiles to be available to common search engines by default and considers certain categories of personal information as "Everyone" information that does not have any privacy settings and protection.[98] This raises questions as to whether individuals have actually consented to disclosure, as well as whether social networks have complied with Article 17 of the E.U. Data Protection Directive (described above) requiring them to implement appropriate technical and organisational measures to prevent unauthorised processing.[99]

## 'Everyone' by default

When Facebook was initially launched, only members could search for other members. On September 5, 2007, Facebook announced that it had made limited public search listings available to people who are not logged into the Facebook website. These search listings expose members' names, profile pictures, the ability to send a message to a member, view his or her friends, and request to add that member as a friend.[100] Facebook also announced that it will make these listings available on search engines such as Google, MSN Live, and Yahoo, which of course, soon after September 5, 2007, did happen.[101] Facebook did not send any email notices to its users notifying them that their listings had become publicly available and or that Facebook users' information is set to 'Everyone' by default. Indeed, Facebook announced through its blog that it does not have a policy of notifying users of changes to the site via email.[102]

Carolyn Abram, Facebook's "resident blogger," explained there are only four ways that Facebook sends information to users[103]: through Home Page announcements, Product Stories and the What's New page, the Facebook Blog, and Pages and Updates. Home Page announcements are "big boxes" that appear at the top of a user's News Feed when that user logs into Facebook. Abram explained that Home Page announcements are used only for the announcements that Facebook wants to be sure its users are aware of.[104] Product Stories and the What's New page appear as stories on users' News Feeds and are used to communicate "useful tips and fun information about Facebook." Finally, Pages and Updates appear in users' message inboxes, which they can access after logging into the website. After the public search change that Facebook Inc., decided arbitrarily, all users were automatically included in the public search listings; they were given the option to opt-out of the public listings, but of course said option was offered after the fact of being publicly listed, via Facebook's individualized privacy settings page.[105] Before Facebook's move to make its search listings public and available on search engines such as Google, MSN Live, and Yahoo there had been no amendment to

Facebook's privacy policy to cover the implications of public searches, but rather only a phrasing included in the Facebook principles[106] stating that "Please keep in mind that if you disclose personal information in your profile or when posting comments, messages, photos, videos, Marketplace listings or other items, this information may become publicly available."[107]

Currently, Facebook Privacy Policy specifically notes that user information may be made public. It states that "Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings. You can, however, limit the ability of others to find this information through search using your search privacy settings."[108] And it also reminds its users that "Some of the content you share and the actions you take will show up on your friends' home pages and other pages they visit. If another user tags you in a photo or video or at a place, you can remove the tag." But this tag-removing activity can, of course happen only after the photo is already published. It also states that "You can also limit who can see that you have been tagged on your profile from your privacy settings." But this limitation is not applicable to a photo published by a friend of a user who has opted for different privacy settings than the user's settings.[109] Facebook explicitly admits that "Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings, or it was copied or stored by other users." That is to say that information removal might be totally ineffective for a user since in almost all cases postings of information in one place are viewable in many others, and users tend to re-post elsewhere information they like.[110] And that a user understands "…that information might be reshared or copied by other users." And since a user understands this as a standard process and still consents to the use of the Facebook Platform, there's limited room to object to it through any applicable and sustainable legal action against Facebook Inc.

Facebook's decision to make public search listings available initially generated some user protest,[111] but that protest quickly waned.[112] This may be because creating a profile, which gives access to Facebook user information, requires so little effort. Because establishing membership is very easy, many members do not see a fundamental difference between opening Facebook up to public membership, and allowing non-members to search Facebook profiles. However, Facebook's announcement that it would make public listings available to users of search engines was a dramatically new and unprecedented development in the world of social networking websites.[113] It may not be a decision that members felt they agreed to when they read and accepted the website's privacy policy.[114] Yet, their protests against making listings publicly

available were not loud enough to make Facebook Inc. retreat from putting their users' personal and sensitive data at anyone's access and retrieval.

Additionally, the developers behind the Facebook applications are also largely invisible, obscuring the fact that the information is in fact leaving the confines of Facebook and not just going to the user's friends. Applications run within the boundary of the site, giving users the impression that they are interacting with Facebook and others on Facebook.[115] Yet, this effectively obscures the fact that they are also interacting with some third party server on which Facebook Inc. and Facebook Platform have no power and probably the Facebook application developer has no full power upon, too.[116] Moreover, users are not aware of the fact that all of the other personal information on their profile as well as personal and sensitive data and information of their friends' profiles are potentially being accessed by those third party application developers for who Facebook Inc. waives its legal responsibility acknowledging bluntly in fact the company's inability to control the behaviour of third party Facebook Application developers regarding the use of Facebook users' personal and sensitive data and information.[117] The result is that users have little understanding of the information they are sharing, with whom they are sharing it, and that they are responsible for sharing—leaking, actually—all of their friends' personal and sensitive data and information as well.[118]

## Invisibility of information flows via Facebook

Facebook Privacy Policy provisions clearly indicate that any information members provide may become "publicly available." Facebook users do not have a subjective expectation of privacy in their profiles, since the very purpose of creating a Facebook profile is to make information available to others. Even though the privacy policy may not be a binding agreement, it still seems odd for a Facebook member to expect notice before his or her information is made publicly available when all members are required to agree to a privacy policy that specifically states that user information may be made publicly available. The invisibility of information flows presents a particular problem because when a user does not know what is being done with her information, she has no ability to contest it. If the architecture and interface of Facebook essentially hides the amount of information that is shared to third parties, then there is little that a user can do about that sharing.

Indeed, there is little that she can do to avoid the situation, other than decline to use the third party applications or Facebook per se. The choice for a user is binary: install the application and give full access to her own and her friends' personal information, or don't use the application at all.[119] If a user opts for installing a Facebook application then said user technically consents to participating in Facebook and the certain Facebook application when she signs up. But is

questionable whether that consent is adequate in terms of the Law, especially in consideration of the meaning of consent in data-protection E.U.-members regulation. Especially, one of the issues will be whether the consent was obtained under circumstances where the user understands what she's agreeing to.

## New behavioral problems and the "shrinking perceived audience"

In addition, Facebook's architectural design poses us with new behavioural problems which seem to be quite difficult to cope with and come to a satisfactory solution leveraging on any data-protection legislation either in the U.S. or in the E.U. In offline life when dealing with a friend or a small group of them we tend not to perceive said friend or friends as being a number of a much bigger group of friends and peers. Instead, we focus on them and share personal data, beliefs and experiences with them with the perceived assurance that this friendly interaction is bounded by the limits of the participating friends. This behavioural norm affects friendly interactions in the online environment of Facebook, too, despite the fact that Facebook environment is totally different to offline friendly reciprocal communication. Though users tend to shake-hands with as many Facebook friends as possible, they also tend to operate periodically with a limited number of them in mind. One can hardly cope with some hundreds or thousands of friends daily regarding personal information and matters other than business and professional activities. After all, one's own life is not an issue to discuss with hundreds or thousands of people simultaneously unless said person is a public persona. Thus, most Facebook users tend to operate with a "shrinking perceived audience."[120] That is, they initially begin by friending a large number of people, and assuming that everything they say is more or less public. Most Facebook users tend to accept friend requests without checking their authenticity or suitability.[121] Over time, though, and as their active in mind circle of friends narrows, they tend to forget about the earlier friends, who are still active in the Facebook Platform and/or Applications, and tend to focus on the narrower cycle of the active friends only, but even when acting with them in mind, neither do they tend to perceive that their Facebook postings is a topic for discussion among all of their active—in mind, moreover in Facebook Platform—friends nor that any updates to their earlier discussions remain available permanently to be seen and used by any of their Facebook friends. The News Feed format also encourages this thought, since updates show up on one's list, only to be displaced shortly thereafter by other updates. One's experience, then, is of ephemeral news postings, not a permanent record. But the record is nonetheless permanent by default;[122] it is possible to go back and view all of a person's updates over a period of several years unless she deletes them.[123]

The behavioural norm of offline friendly interaction is a pattern that crops up subconsciously because it is manageable. Yet, this norm of offline friendly interaction is not a pattern applicable to the online environment of Facebook as we've presented hereto. Every posting of a user becomes public to a user's friends either they are active or not. Thus, every personal data, and every newsfeed from a user's personal and/or professional life becomes a topic for discussion for any user's Facebook friend. Additionally, Facebook's architectural design aims at promoting multilateral rather than bilateral communication. Facebook's multilateral communication technologies and their interfaces can facilitate some values and behaviors at the expense of others such as one-to-one communication. Even when communication feels to be bilateral, in fact it is not. For example, 'wall-to-wall' communications allow one to exhange messages with a single friend asynchronously in what feels and looks like a private space, but which is in fact visible to others. The abstraction involved in asynchronous, online social networking encourages a gap between a user's perceived audience and the actual audience. Users tend to significantly under-perceive the size and scope of the audience for their postings.[124] The multilateral communication of Facebook's architectural design is constantly evolving as the technology of social networking sites enables entire types of interactions that are not available offline. Changes in the interface affect how people behave online, and those behavioral changes feed back into the norms that guide them.

## Facebook Social Ads

Among the applications that were announced[125] in 2007 with the aim to enhance Facebook's social networking experience was what it called "an entirely new advertising solution for Facebook", i.e. Social Ads. Social ads display relevant advertisements related to actions that users have taken on the site.[126] The announcement specified that the new Social Ads product would result in three main changes for Facebook users: (1) it would give users a way to connect with "products, businesses, bands, celebrities and more"; (2) ads would become "more relevant and more meaningful" to users; and (3) users would have the options to share actions they take on third-party websites with their Facebook friends. Facebook assured users that advertisers would never have access to who is seeing their ads, personal information about users, or the social actions that accompany their ads, but rather that only friends of a user would share the personally identifiable information visible in a social ad.[127] This announcement was only published in the Facebook blog, though in accordance with Facebook policy, no announcements were sent to users' personal email addresses.[128] Also, though Facebook Inc. acknowledges data sharing, commonly known as "conversion tracking"[129] that helps the company to measure its advertising effectiveness and improves the quality of the advertisements that Facebook users see, it does not provide through the Facebook Privacy Policy any

clarification upon the method it uses in the conversion tracking process.[130] And though Facebook Inc. states that it does not share its users' personal data with advertisers, yet it does state that the company allows advertisers to choose the characteristics of users who will see their advertisements through Facebook based on any of the non-personally identifiable attributes[131] of Facebook users that Facebook Inc. has collected and shared with advertisers including information that users may have decided not to show to other users, such as their birth year or other sensitive personal information or preferences.[132] It is obvious that Facebook Inc., despite any different claims, it does leverage on personal data and information submitted to Facebook Platform by its users with the aim to profit from the exchange of this information. There are advertising methods such as the 'behavioral targeting' which are used in order to produce the maximum financial gains for the (right)-holder of this information.[133] Personal and sensitive data and information submitted into the Facebook system is treated as if it were a corporate asset; software development is using said data and information with the aim to make the most out of it, as well as make most users submit through the Facebook Platform as more data and information as possible.

## Problematic and biphasic privacy in the nook of Facebook

In consideration of the analysis described hereto, it is beyond any doubt that privacy in the nook of Facebook currently is problematic and biphasic, at least. Biphasic is in the sense that by 2005 it started as data and information available to no one but a user and his/her friends unless said user decided otherwise, while by 2009 it turned into data and information available to everyone unless a user decided it to be only for him/her and his/her friends. And problematic is in any E.U. sense of privacy and data protection. Facebook's disrespect for privacy norms is reflected in the company's chief executive officer's publicly stated views. Facebook's founder and CEO Mark Zuckerberg has no hesitation in making public statements of his views that the age of privacy is over[134] or that what people want isn't complete privacy[135] or that he sees no reason why information in people's accounts, as in his own Facebook account, should not be public and accessible to everyone,[136] or in making assertions that people may be more excited about exposing their life-activities such as shopping records in a few years rather than keep these activities under the privacy hood.[137] Yet, he does recognize that privacy is an issue of focal point for Facebook.[138]

The current situation in Facebook is one of legal uncertainty—if not of legal confrontation and direct breach of data protection law in the E.U. legal environment—which causes problems for both regulators and individuals whose privacy and personal data are not fully protected.[139] Because of this fact as well as in consideration of the fact that national Authorities[140] as well as international European Authorities[141] have already pointed out the conflicts of social networking

sites and practices with the local and the E.U. data protection legal framework with the aim to make Facebook and other social networking sites to comply with the local and the E.U. data protection law,[142] in my opinion Facebook Inc.—the biggest and most popular social network operator—is faced with an eerie, major, and multi-dimensional crisis. The first signs of this crisis for Facebook Inc. are already discernible through the press and the media.[143] Facebook is met more-and-more with bud publicity periodically regarding data-protection and privacy through the company's Platform and third-party Applications.[144] If the management of Facebook Inc. does not decide to change its current Privacy Policy and reshape the Facebook Platform and/or Applications accordingly so as to comply with data protection legal frameworks that put an emphasis on the protection of individual's privacy rights, i.e. to provide settings that restrict access to Facebook users profiles to a user's own self-selected contacts, as well as settings that require user's affirmative consent in the meaning of prior free and unambiguous consent of the data subjects as said consent is defined in E.U. data protection legislation before any profile is accessible to third parties; if they don't opt for settings that provide restricted access to users' profiles so that they are not discoverable by internal/external search engines. If not that minimum but necessary for data protection and privacy compliance changes do not happen any time soon, if not Facebook Inc. make all necessary changes in its Platform and third-party admittance Applications policy so that users have full command of their personal data and information, then Facebook Inc. would probably have to face a litigation spree, that is to say legal measures with possible severe consequences, taken against it either by national Authorities, European Authorities or E.U.-members' Authorities and/or Facebook users in the form of class action suites, too. For Facebook Inc., a possible implication of this kind is not only a crisis of litigation nature, but could possibly, also, turn into a public relations and corporate public affairs crisis regarding the company's reputation and other intangible assets of it with negative consequences on the company's tangible assets and their traded value.[145]

The value of Facebook lies not just in the content provided (which is group-specific), but in its replication in electronic form of the web of human relationships and trust connections. Therefore, possible litigation based on breaches of privacy and data-protection legislation is a direct hit to the core of trust-relationships and connections which Facebook Inc. purports to support, and which is a necessary ingredient in the Information Society.[146] Facebook and all social networking sites may be seen as informal but all-embracing trusted identity management tools,[147] defining access to user-created content via social relationships. If this identity management were found to fail and mistrust because of privacy and data-protection failure, then the identity management tools operator would reasonably be expected to fail and mistrust, too, unless serious effort were undertaken with the aim to comply

with data protection legal frameworks in consideration of which the identity management tool operator could be judged. Said legal frameworks may also need to be modified or extended aiming at ruling clearly the operation of Facebook and other social networking services which represent a relatively novice phenomenon.[148] Especially, differing legal frameworks which affect the operation and development of social networking sites through their provisions for the protection of privacy, personal and sensitive data of data subjects, such as the U.S. from one side and the E.U. from another, might need to be re-examined with the aim to adopt unified ruling on basic privacy, data protection principles and core data subject's rights. Negotiations aiming at that point have already started between the E.U. and the U.S.[149] There is no doubt that Facebook and the peer social networking sites present a scenario, which was hardly foreseen clearly when current data-protection legislation was created. This means that certain issues in data-protection law may, also, need to be clarified.[150] But, it also means that Facebook Inc. under current legislative framework for data protection and privacy certainly needs to change its Platform and Applications so that it abides by law. It remains to be seen.

## Endnotes

1. Mitrou, L., (2010), Protection of Privacy in Information and Communication Technologies—The Legal point of view, in Protection of Privacy & Information and Communication Technologies—Technical and Legal issues, Labrinoudakis, K., Mitrou, L., Gritzalis, S., Katsikas, S., eds., Papassotiriou publications; Mitrou, L., and Karyda, M., (2006), Employees' Privacy vs. Employers' security: can they be balanced?, Elsevier, Telematics and Informatics 23(2006); Slobogin, C., (2002), Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity, Mississippi Law Journal 72(2002), available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=364600 [last access, Jun.5, 2010]. On different facets of Bottis M., The protection of private life and european legislation on data protection. Honorary Volume for M. Stathopoulos, Sakkoulas 2009, 809-823.
2. Bygrave, L., (2004), Privacy Protection in a Global Context—A Comparative Overview, Published in Scandinavian Studies in Law, 47(2004), 319-348, available at http://folk.uio.no/lee/publications/Privacy%20in%20global%20context.pdf [last access, Jun.5, 2010]; Whitman, J., (2004), The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 Yale Law Journal 1151 (2004), available at http://www.yalelawjournal.org/images/pdfs/246.pdf [last access, June 5, 2010].
3. Nissenbaum, H., (2004), Privacy as Contextual Integrity, Washington Law Review 79, 101-139, available at http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf [last access, June 5, 2010]; Hull G., Lipford H. R., Latulipe C., (2009), Contextual Gaps: Privacy Issues on Facebook, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1427546 [last access, June 5, 2010]; Cohen, J.E., (2000), Examined Lives: Informational Privacy and the Subject as Object, Georgetown Public Law Research Paper No. 233597, available at http://ssrn.com/abstract=233597 [last access, June 5, 2010]. For the extended and (re)shaped meaning of privacy in public and/or in private spaces, see Mitrou, L., (2010), ibid.

4. In Europe, the protection of individuals with regard to the collection, processing, use and movement of personal data is covered by the European Parliament and Council Directive 95/46/EC of October 24, 1995, or the Data Protection Directive (Directive 95/46/EC of the European Parliament 1995) (See the Data Protection Directive at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf [last access, Jun.5, 2010]). The processing of personal data and the protection of privacy in the electronic communications sector are the subject of Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, or the Directive on Privacy and Electronic Communications (Directive 2002/58/EC of the European Parliament 2002) (See the Directive on Privacy and Electronic Communications at http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf [last access, June 5, 2010]), which extends privacy protections to unsolicited commercial e-mail, telephone communications, requires websites to disclose the use of cookies, and recommends that privacy notices are short and easy for consumers to understand. The Directive on Privacy and Electronic Communications was amended by Directive 2009/136/EC of the European Parliament and of the Council of November 25, 2009 See the Directive 2009/136/EC at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF [last access, Jun.5, 2010]).
5. Facebook Inc., is based in the State of California. The international headquarters of Facebook is based in Dublin wherefrom Facebook Inc., will provide a range of online technical, sales and operations support to Facebook's users and customers across Europe, the Middle East and Africa. The company refrains from clarifying what is the nature of said support and the services provided to E.U. citizens from its international headquarters in Dublin. See more at Press Release, Facebook to Establish International Headquarters in Dublin, Ireland, October 2, 2008, available at http://www.facebook.com/press/releases.php?p=59042 [last access, June 5, 2010].
6. Facebook Inc. subjects to the E.U. data protection law because of article 4 of the E.U. Data Protection Directive (Directive 95/46/EC) and according to Article 29 Data Protection Working Party's interpretation of said clause. Article 4 of the Directive reads as follows: §1. Each Member State shall apply the national provisions it adopts pursuant to 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; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; (b) 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; (c) 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 State, unless such equipment is used only for purposes of transit through the territory of the Community. §2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions, which could be initiated against the controller himself. Also, see Article 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, WP 148/00737/EN, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf [last access, June 5, 2010]; the same, Working document on determining the international application of E.U. data protection law to personal data processing on the Internet by non-E.U. based

websites, WP 56/5035/01/EN/Final, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf [last access, June 5, 2010].

7. Birnhack, M., (2008), The EU Data Protection Directive: An Engine of a Global Regime, Computer Law & Security Report, Vol. 24, No. 6, 2008, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1268744 [last access, June 5, 2010]; Burk., D., (2005), Privacy and Property in the Global Datasphere, Minnesota Legal Studies Research Paper No. 05-17, available at http://ssrn.com/abstract=716862 [last access, June 5, 2010].

8. Solove, D. J., (2002), Conceptualizing Privacy, California Law Review, 90, 1087, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103 [last access, June 5, 2010]. Even in the E.U. legal environment for personal and sensitive data protection, privacy may have different flavours such as the right to be let alone, the right to shield oneself from unwanted access by others, the right for concealment of certain matters from others, the right to control over personal information, and the right to protect one's personality, individuality, and dignity. See, also, Jones, H., and Soltren, J.H., (2005), Facebook: Threats to privacy, Project MAC: MIT Project on Mathematics and Computing. For the meaning of Privacy in the E.U. legal framework, see also, the European Court of Human Rights case Botta v. Italy (153/1996/772/973) February 24, 1998, available at http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=696017&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166 [last access, June 5, 2010], the European Court of Human Rights case Gaskin v. United Kingdom (10454/83) July 7, 1989, available at http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=695368&portal=hbkm&source=externalbydocnumber [last access, June 5, 2010]; the European Court of Human Rights case Guerra and Others v Italy (116/1996/735/932) February 19, 1998, available at http://www.iidh.ed.cr/comunidades/libertadexpresion/docs/le_europeo/guerra%20and%20others%20v.%20italy.htm [last access, June 5, 2010]; see also, Mitrou, L., (2010), ibid.

9. By May 2010, Facebook has become a community of more than 400 million users—almost 500 users. See Zuckerberg, M., (2010), From Facebook, answering privacy concerns with new settings, Wall Street Journal, May 24, 2010, available at http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html [last access, June 5, 2010]; Fletcher, D., (2010), Facebook Society—Friends Without Borders, Time magazine, May 31, 2010, p.18-24, cover page of Time magazine issue of May 31, 2010, under the title Facebook …and how it's redefining privacy, available at http://www.time.com/time/business/article/0,8599,1990582,00.html [last access, June 5, 2010], according to which within the next few weeks (of June-July 2010), Facebook will officially log its 500 millionth active citizen. If the website were granted terra firma, it would be the world's third largest country by population, two-thirds bigger than the U.S. More than 1 in 4 people who browse the Internet not only have a Facebook account but have returned to the site within the past 30 days.

10. Except Facebook, other social networking sites include ARTO (http://www.arto.com [last access, June 5, 2010]), BEBO (http://www.bebo.com [last access, June 5, 2010]), DAILYMOTION (http://www.dailymotion.com/gr [last access, June 5, 2010]), GIOVANI.IT (http://www.giovani.it [last access, June 5, 2010]), HYVES.NL (http://www.hyves.nl [last access, June 5, 2010]), MYSPACE (http://www.myspace.com [last access, June 5, 2010]), NASZA-KLASA.PL (http://nasza-klasa.pl [last access, June 5, 2010]), NETLOG (http://www.netlog.com [last access, June 5, 2010]), ONE.LT (http://w29.one.lt/welcome [last access, June 5, 2010]), PICZO (http://www.piczo.com/?cr=3 [last access,

June 5, 2010]), RATE.EE (http://www.rate.ee [last access, June 5, 2010]), SKYROCK.COM (http://www.skyrock.com [last access, June 5, 2010]), SULAKE (http://www.sulake.com [last access, June 5, 2010]), TUENTI (http://www.tuenti.com/?m=login [last access, June 5, 2010]), VZNET NETZWERKE LTD. (http://www.meinvz.net/Default [last access, June 5, 2010]),, ZAP.LU (http://www.zap.lu [last access, June 5, 2010]).

11. danah michele boyd, a social media researcher and fellow at Harvard University's Berkman Center for Internet and Society has preference in writing and using her name without any capitalization of her name. Her decision to leave capitalization out of her name is respected, thus any references here to to her name in consideration of citation to her work will leave capitalization out. See more about her preference regarding writing her name at http://www.danah.org/name.html [last access, June 5, 2010].
12. boyd, d., and Ellison, N., (2007), Social Networking Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication, 13(1), available at http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html [last access, June 5, 2010].
13. Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136/01248/07/EN, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf [last access, June 5, 2010].
14. ENISA Position Paper No.1, (2007), Security Issues and Recommendations for Online Social Networks, ed. Giles Hogben, available at http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks [last access, June 5, 2010].
15. Hull G., Lipford H. R., Latulipe C., (2009), ibid.; West, A., Lewis, J., and Currie, P., (2009), Students' Facebook 'friends': public and private spheres, Journal of Youth Studies, 12(6), 615-627; Zhao, S., Grasmuck, S., and Martin, J., (2008), Identity construction on Facebook: Digital empowerment in anchored relationships, Computers in Human Behavior, 24(5), 1816-1836.
16. boyd, d., (2008), Taken out of context: American teen sociality in networked publics, University of California at Berkeley, available at http://www.danah.org/papers/TakenOutOfContext.pdf [last access, June 5, 2010]; Marwick, A., Diaz, D. M., and Palfrey, J., (2010), Youth, Privacy and Reputation, Research Publication 2010-5, The Berkman Center for Internet and Society at Harvard University, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163 [last access, June 5, 2010].
17. Facebook Statement of Rights and Responsibilities, 4.Registration and Account Security, available at http://www.facebook.com/#!/terms.php?ref=pf [last access, June 5, 2010]. The online collection of personal information from children under 13 years old by persons or entities under the U.S. jurisdiction is illegal according to Children's Online Privacy Protection Act (COPPA) of October 1998, 15 U.S.C. §§ 6501–6506 (2006). Companies operating websites that fall outside COPPA's jurisdiction but still target young people remain under the watch of the Federal Trade Commission (FTC), which has the authority to enforce the commitments made to Internet users under privacy policies under the FTC's general unfair and deceptive practices powers. Since 1998, the FTC has maintained the position that the use or dissemination of personal information in a manner contrary to a posted privacy policy is a deceptive practice under the FTC Act Section 45(a)(1).

18. Gross, E.F., (2004), Adolescent Internet use: What we expect, what teens report, Journal of Applied Developmental Psychology, 25(6), 633-649. According to this study, about half of the 175 7th and 10th graders in her survey had pretended to be someone else online, but of that, almost all had pretended to be older. See, also, Steeves, V., and Webster, C., (2008), Closing the barn door: the effect of parental supervision on Canadian children's online privacy, Bulletin of Science, Technology and Society, 28(1), 4-19, who report that the majority (59%) of their 3,000 respondents had, at one time, pretended to be a different age (52%), a different personality (26%), or someone with a different physical appearance (23%). Respondents said they did this for a variety of reasons, including seeing what it would be like, to flirt, to pretend to be older, or to act "mean." More research findings at Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid.
19. Lwin, M.O., Stanaland, A.J., and Miyazaki, A.D., (2008), Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness, Journal of Retailing 84(2), 205-217.
20. Online fights using electronic messages with angry and vulgar language.
21. Setting up accounts pretending to be people in order to humiliate them; sending or posting gossip or rumors about a person to damage his or her reputation or friendships.
22. Pretending to be someone else and sending or posting material to get that person in trouble, and put them in danger or to damage their reputation or friendships.
23. Sharing someone's secrets or embarrassing information or images online.
24. Talking someone with the aim to make her into revealing secrets or embarrassing information, and then sharing it online.
25. Intentionally and cruelly excluding someone from an online group as a form of punishment.
26. Typically linked to a problematic intimate relationship, repeated, intense harassment and denigration that includes threats or creates significant fear.
27. ENISA Position Paper No.1, (2007), ibid.
28. Ito, M., Horst, H., Bittanti. M., boyd D., Herr-Stephenson, B., Lange, P., Pascoe, C., and Robinson L., (2008), Living and Learning with New Media: Summary of Findings from the Digital Youth Project, The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning, 52, available at http://www.macfound.org/atf/cf/%7BB0386CE3-8B29-4162-8098-E466FB856794%7D/DML_ETHNOG_WHITEPAPER.PDF [last access, June 5, 2010].
29. Steeves, V., and Webster, C., (2008), ibid. There are research findings, though, that reach different conclusions regarding privacy-protective behavior. Two-large scale studies concluded that slightly less than half of users set their social network profile to private, making it inaccessible to anyone outside their group of friends. See more at Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid.; Hinduja, S., and Patchin, J.W., (2008), Personal Information of adolescents on the Internet: A quantitative content analysis of MySpace, Journal of adolescence, 31(1), 125-146; Lenhart, A., and Madden, M., (2007), Teens, Privacy and Online Social Networks, Washington DC: Pew Internet and American Life Project, available at http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Privacy_SNS_Report_Final.pdf.pdf [last access, June 5, 2010].
30. Valkenburg, P.M., and Peter, J., (2008), Adolescents' identity experiments on the Internet: Consequences for social competence and self-concept unity, Communication Research, 35(2),

208; Govani, T., and Pashley, H., (2007), Student awareness of the privacy implications when using Facebook, Carnegie Mellon University, available at http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf [last access, June 5, 2010]. See, also, Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid. for further references to related research findings; Tuunaimen, V.K., Pitkanen, O., and Hovi, M., (2009), Users' Awareness of Privacy on Online Social Networking sites—Case Facebook, 22nd Bled eConference eEnablement: Facilitating an Open, Effective and Representative eSoceity, available at http://ecom.fov.uni-mb.si/proceedings.nsf/0/9b675b5e811394f0c125760000390664/$FILE/1_Tuunainen.pdf [last access, June 5, 2010]. But, more recent reports find that privacy-protecting activities have become considerably more common across all age groups than they were when similar studies were conducted in the past. For example, see Madden, M., and Smith, A., (2010), Reputation Management and Social Media, How People monitor their identity and search for others online, May 26, 2010, Pew Internet & American Life Project, available at http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management.pdf [last access, June 5, 2010] which indicates that a relative lack of concern about the availability of personal information online does not necessarily translate into inaction. Indeed, many of the least concerned Internet users have still taken steps to restrict what they share with others. For example, two-thirds of all social networking users (65%) say they have changed the privacy settings for their profile to limit what they share with others online. Among social networking users who worry about the availability of their online information, fully 77% have changed their privacy settings. However, even those who don't worry about such information are relatively active in this regard—59% of these less concerned social networking users have adjusted their privacy settings in this way.

31. Livingstone, S., (2005), Mediating the public/private boundary at home, Journal of Media Practice, 6(1), 11-151; Steeves, V., and Webster, C., (2008), ibid.; Levin, A., and Abril, P.S., (2009), Two Notions of Privacy Online, Vanderbilt Journal of Entertainment and Technology Law, v.11, 1001-1051, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1428422 [last access, June 5, 2010].

32. Aidman, A., (2000), Children's Online Privacy—What you Need to Know about the Children Online Privacy Protection Act, Educational Leadership 58(2), 46-48; Giffen, M., (2008), Online Privacy, Current Health, 34(7), 8-11; Palfrey, J., Gasser, U., (2008), Born Digital: Understanding the First Generation of Digital Natives, New York Basic Books; Palfrey, J., Sacco, D., boyd, d., (2008), Enhancing Child Safety and Online Technologies: Research Advisory Board Report for the Internet Safety Technical task Force, Cambridge MA: The Berkman Center for Internet and Society at Harvard University; Youn, S., (2009), Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents, Journal of Consumer Affairs, 43(3), 389-418; Lenhart, A., and Madden, M., (2007), ibid.

33. Grimmelmann, J., (2009), Saving Facebook, Iowa Law Review, 94 (1137).

34. Hull G., Lipford H. R., Latulipe C., (2009), ibid.

35. Christofides, E., Muise, A., and Desmarais, S., (2009), Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?, CyberPsychology & Behavior, 12(3), 341-345; Debatin, B., Lovejoy, J., Horn, A.K., and Hughes, B., (2009), Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences, Journal of Computer-Mediated Communication, 15(1), 83-108.

36. Weibel, P., (2002), Pleasure and the Panoptic Principle, CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother, ed. Thomas Y. Lenin et. al. Cambridge MA MIT Press, 206-223.
37. Gross, R., and Acquisti, A., (2005), Information Revelation and Privacy in Online Social Networks (The Facebook case), ACM Workshop in Privacy in the Electronic Society (WPES).
38. Christofides, E., Muise, A., and Desmarais, S., (2009), ibid.
39. See, for example, how respected blogger Will McInnes explains Facebook users' stance regarding their privacy through Facebook, in Brown, B., (2009), Net guru on Facebook data policy, video BBC News, February 18, 2009, available at http://news.bbc.co.uk/2/hi/technology/7897824.stm [last access, June 5, 2010].
40. West, A., Lewis, J., and Currie, P., (2009), ibid.
41. Studies of identity construction on Facebook have found that people construct strategic identities that reflect their social wannabes. See Liu, H., (2007), Social network profiles as taste performances, Journal of Computer-Mediated Communication, 13(1), 252; Zhao, S., Grasmuck, S., and Martin, J., (2008), ibid.
42. Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid. refer to this publicity quest as 'micro-celebrity' identity construction that is presented to one's audience in Facebook and is most likely constructed with the audience in mind, emphasizing qualities considered high-status within that community and de-emphasizing attributes that are not characteristic of the publicity-seeker's environment.
43. That explains why people who leverage on publicity with the aim to make profit tend to flock in Facebook and other social networking media, daily. There are many examples for this tendency of professionals such as lawyers, especially young ones with an insentient thirst to become known, who post onto Facebook any kind of information, relevant or irrelevant, to their professional activities, stupid or not, aiming at attracting the eyeballs of any Facebook user who could support their self-publicity cause. Research indicates that the use of social network sites, which require the sharing of personal information, allows young people to maintain weak ties, strengthen friendships, increase social capital, and gain popularity (e.g. see Ellison, N., Steinfield, C., and Lampe, C., (2007), The Benefits of Facebook 'friends': social capital and college students' use of online social network sites, Journal of Computer-Mediated Communication, 12(4), 1143; Joinson, A.N., (2008), Looking at, looking up or keeping up with people?: motives and use of Facebook, CHI Proceedings—Online Social Networks). This publicity quest of young professionals reminds me Oscar Wild's cynical saying "The only thing worse than being talked about is not being talked about." Yet, aside from this consideration, the posting onto Facebook of any nook and cranny of a lawyer's life, especially of information pertaining to his/her professional life and clients, is of questionable legality, especially in relation to Lawyer's Code of Conduct, i.e. Law 3026/1954 for Lawyers in Greece as it stands now—one could predict that this law will soon be amended so that lawyers are allowed to advertise themselves, but no amendment is predicted regarding a lawyer's obligation not to reveal to any third party matters upon his/her clientele. Said public speaking upon a lawyer's professional life through Facebook is, also, profoundly, provocative, and indicative of a lack of professionalism as well as lack of any sense of privacy protection. Information posted onto its Platform will become public. And once this information is public none can say how this information will be handled and used by any third party. The inability to describe how information provided online will

be handled and used is referred to as "information risk". Though studies repeatedly have shown that "information risk" increases concerns over privacy when users do not know how their personal information will be used (e.g. see Youn, S., (2009), ibid.; Sheehan, K.B., and Hoy, M.G., (1999), Flaming, complaining, abstaining: How online users respond to privacy concerns, Journal of Advertising, 28(3), 37-51), and though that increased "information risk" increases the likelihood of a person adopting privacy-protecting behaviors, yet lawyers who do exactly the opposite by posting every aspect of their (professional) life onto Facebook with the aim to become known and be talked about do nothing more than bluntly self-advertise in a rather stupid and amateurish way and self-promote either ignorance and naivety or disrespect in terms of data protection, at least. On the other hand, decisions taken by Bar Associations such as the Athens Bar Association's decision of May 20, 2009, (see the decision at http://www.dsa.gr/index.phtml?url=news&categ=%CD%DD%E1-%C1%ED%E1%EA%EF%E9%ED%FE%F3%E5%E9%F2&id=417113&search=yes&searchkeywords=Internet [last access, June 5, 2010]) with the aim to restrict lawyers' use of the Internet do not make any sense because 1) decisions can hardly be imposed on the Bar Association's members; 2) decisions are wrong to the point that they consider the Internet as merely an advertising medium; the Internet and Internet applications are much more than that; 3) though said decisions consider lawyers' online behavior which might be in conflict with Lawyer's Code of Conduct which currently forbids lawyers' advertising, yet, in most cases, criticized lawyers' behavior online might not be an issue of direct and/or indirect advertising or any other issue of professional standards in accordance with current legislation, but rather it might be a matter of lack of common sense as well as bad aesthetics in their presence online; while Bar Associations are organizations appropriate to instruct on professional standards, yet they are not appropriate to command on common sense and aesthetics.

44. ChoicePoint, one of the largest data brokers in the world, in early 2005 admitted that it had released sensitive data on roughly 163,000 people to fraudsters who signed up as ChoicePoint customers starting in 2001. At least 800 cases of identity theft resulted. Sued by the FTC, the company paid USD $15 million in a settlement by 2006, at least USD $5 million of which went to the consumers whose lives they ruined. See more at http://www.wired.com/politics/security/news/2006/08/71622#ixzz0oNuTAjQx [last access, June 5, 2010]; in February 2008, ChoicePoint was purchased by Reed Elsevier for 3.6 billion USD $. See more about ChoicePoint at Wikipedia at http://en.wikipedia.org/wiki/ChoicePoint [last access, June 5, 2010].

45. Digital dossiers of personal information may result in cases of discrimination against individuals based on their personal data or in cases of identity theft, stalking, harassment, and other invasions of privacy. See more at Ciocchetti, C., (2007), E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors, American Business Law Journal 44(1), 55-126; Palfrey, J., and Gasser, U., (2008), ibid.; ENISA Position Paper No.1, (2007), ibid.

46. Solove, D., (2004), The Digital Person: Technology and privacy in the information age, New York University Press.

47. Xie, E., Teo, H., and Wan, W., (2006), Volunteering personal information on the Internet: Effects of reputation, privacy notices, and rewards on online consumer behavior, Marketing Letters, 17(1), 61-74; Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid.; Hendry, J., and Goodall, K., (2010), Facebook and the Commercialisation of Personal Information: Some Questions of Provider-to-User Privacy, in M.E.A. Goodwin, B.J. Koops and R.E. Leenes, eds., Dimensions of Technology Regulation, Wolf Legal Publishing.

48. Peterson, C., (2010), Losing Face: an Environmental Analysis of Privacy on Facebook, available at http://etc.cpeterson.org/research/workingpapers/2010/losingface_workingpaper.pdf [last access, June 5, 2010].
49. Face-recognition technology is used with the aim to identify a Facebook user who though she posts—or any third party posts—online a photograph of herself, she uses pseudo-anonymous profile. See ENISA Position Paper No.1, (2007), ibid.
50. Content-based Image Retrieval (CBIR) is an emerging technology which can match features, such as identifying aspects of a room (e.g. a painting) in very large databases, increasing the possibilities for locating users. See ENISA Position Paper No.1, (2007), ibid.
51. Many SNSs now allow users to tag images with metadata, such as links to SNS profiles (even if they are not the owner/controller of that profile), or even e-mail addresses. This leads to greater possibilities for unwanted linkage to personal data. See ENISA Position Paper No.1, (2007), ibid.
52. Unsolicited messages propagated using SNSs. See ENISA Position Paper No.1, (2007), ibid.
53. SNSs are vulnerable to XSS attacks and threats due to 'widgets' produced by weakly verified third parties. See ENISA Position Paper No.1, (2007), ibid.
54. 'SNS portals' integrate several SNSs which multiply vulnerabilities by giving read/write access to several SNS accounts using a single weak authentication. See ENISA Position Paper No.1, (2007), ibid.
55. Cyber-stalking is threatening behavior in which a perpetrator repeatedly contacts a victim by electronic means such as email, Instant Messenger and messaging on SNSs. Statistics suggest that stalking using SNSs is increasing. ENISA Position Paper No.1, (2007), ibid.
56. Cyber-bullying is the behavior of repeated and purposeful acts of harm such as harassment, humiliation and secret sharing. ENISA Position Paper No.1, (2007), ibid.
57. Solove, D., (2004), ibid. He speaks for a 'Kafkaesque world of bureaucracy' where people are vulnerable to exploitation of their personal information and subject to a bureaucratic process that is itself not adequately controlled. See, also, Palfrey, J., Gasser, U., (2008), ibid.
58. Data Protection and Freedom of Information Commissioner of the State of Berlin, Germany, (2008), Resolution on Privacy Protection in Social Network Services, available at http://www.lda.brandenburg.de/sixcms/media.php/3509/resolution_social_networks_en.pdf [last access, June 5, 2010].
59. Hull G., Lipford H. R., Latulipe C., (2009), ibid.
60. boyed, d., (2007), Why Youth (Heart) Social Network Sites: The Role of Networked Publics, in D. Buckingham, ed. Youth Identity and Digital Media, Cambridge MA: MIT Press.
61. Benkler, Y., (2006), The Wealth of Networks: How Social Production transforms Markets and Freedom, Yale University Press, Chapter 10: Social Ties: Networking Together, available at http://cyber.law.harvard.edu/wealth_of_networks/Main_Page [last access, June 5, 2010].
62. Benkler, Y., (2006), ibid.
63. Jones, H., and Soltren, J.H., (2005), ibid.
64. Govani, T., and Pashley, H., (2007), ibid.
65. Hull G., Lipford H. R., Latulipe C., (2009), ibid.
66. Strater K., and Lipford H.R., (2008), Strategies and Struggles with Privacy in Online Social Networking Community, Proceedings of the 22nd British HCI Group, ACM Press, p.111-119.

Solove D., (2007), The Future of Reputation: Gossip, Rumor and Privacy on the Internet, New Haven, Yale University Press.

67. Hashemi Y., (2009), Facebook's privacy policy and its third-party partnerships: lucrativity and liability, Boston University Journal of Science and Technology Law 15, 140-61.
68. Facebook statistics on the use of its Platform and Platform applications, available at http://www.facebook.com/press/info.php?factsheet#!/press/info.php?statistics [last access, June 5, 2010].
69. Goettke, R., and Christiana, J., (2007), Privacy and Online Social Networking Websites; Nissenbaum, H., (2004), ibid.
70. boyd, d., (2008), Facebook's Privacy Trainwreck – Exposure, Invasion, and Social Convergence, available at http://www.danah.org/papers/FacebookPrivacyTrainwreck.pdf [last access, June 5, 2010].
71. Facebook Privacy Policy, How We Share Information states that "Facebook is about sharing information with others — friends and people in your communities — while providing you with privacy settings that you can use to restrict other users from accessing some of your information. We share your information with third parties when we believe the sharing is permitted by you, reasonably necessary to offer our services, or when legally required to do so." Facebook may be seen as a 'digital cocktail party'. In general, the more contacts you have, the more popular you are, and the more influence you have. However, compared with real-world cocktail parties, Facebook members broadcast information much more widely, either by choice or by mistake. See ENISA Position Paper No.1, (2007), ibid.
72. Picker, R., (2009), Online Advertising, Identity and Privacy, The Law School, The University of Chicago Law and Economics, working paper No. 475, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1428065 [last access, June 5, 2010].
73. Opsahl, K., (2010), Facebook's Eroding Privacy Policy: A Timeline, Electronic Frontier Foundation, Deeplinks Blog, available at http://www.eff.org/deeplinks/2010/04/facebook-timeline [last access, June 5, 2010].
74. Opsahl, K., (2010), ibid.
75. See Article 29 Data Protection Working Party, European data protection group faults Facebook for privacy setting change, Press Release of May 12, 2010, available at http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_12_05_10_en.pdf [last access, June 5, 2010].
76. The Fourth Amendment protection posits that an individual has an expectation of privacy where (1) the individual possesses a subjective expectation of privacy; and (2) that expectation is "one that society is prepared to recognize as "reasonable". The opinion of the Supreme Court of the U.S. in *Katz v. United States,* 389 U.S. 347 (1967) available at http://supreme.justia.com/us/389/347/case.html [last access, June 5, 2010] is that "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. *See Lewis v. United States,* 385 U. S. 206, 385 U. S. 210; *United States v. Lee,* 274 U. S. 559, 274 U. S. 563. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."
77. This is the case of what Solove refers to as the "secrecy paradigm." See Solove, D., (2004), ibid.
78. Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid.

79. For the "third-party doctrine" see Solove, D., (2005), A Taxonomy of Privacy, University of Pennsylvania Law Review, 154(3), 477; Palfrey, J., (2008), The Public and the Private at the United States Border with Cyberspace, Mississippi Law Journal 78, 241-294; Kerr, O.S., (2009), The Case for the Third-Party Doctrine, Michigan Law Review 107(561), 561-602, available at http://www.michiganlawreview.org/assets/pdfs/107/4/kerr.pdf [last access, June 5, 2010]; the same, (2009), Defending the Third-Party Doctrine: A Response to Epstein and Murphy, Berkeley Technology Law Journal 24, 1229-1236, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1608013 [last access, June 5, 2010]; Epstein, R.A., (2009), Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations, Berkeley Technology Law Journal 24(3), 1199.
80. Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid.
81. According to the FOIA (See FOIA through the http://www.justice.gov/oip [last access, June 5, 2010]), federal agencies of the U.S. Government generally are required to disclose records requested in writing by any person. The FOIA applies only to federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies. Each State in the U.S. has its own public access laws that should be consulted for access to state and local records.
82. On December 1, 2009, the Electronic Frontier Foundation submitted a complaint for injunctive relief in the U.S. District Court for the Northern District of California, San Francisco Division, against the Department of Defense (DoD), the Central Intelligence Agency (CIA), the Department of Homeland Security (DHS), the Department of Justice (DoJ), the Department of Treasury (DoT), and the Office of the Director of National Intelligence (ODNI) of the U.S. Government, claiming the Plaintiff that the Defendants do not have any legal ground in consideration of FOIA, 5 U.S.C. § 552 for their investigative, surveillance and data-mining practices through social networking sites such as Facebook and MySpace (See the Complaint at http://www.eff.org/files/filenode/social_network/social_networking_FOIA_complaint_final.pdf [last access, June 5, 2010]). The reply to the requested injunctive relief was issued on February 8, 2010 (See the Answer to the Complaint at http://www.eff.org/files/filenode/social_network/social_networking_FOIA_answer_0.pdf [last access, June 5, 2010]), in which almost all Defendants answered that they lack sufficient knowledge or information to admit or deny the allegations of the Plaintiff, i.e. they claim that they do not know whether data-mining for investigative, surveillance or any other purposes is happening. The Court, also, ruled that Defendants rightfully asserted that Plaintiff was not entitled to the relief requested, or to any relief whatsoever, and ruled that Plaintiff's action be dismissed in its entirety with prejudice and that Defendants be given such other relief as the Court deemed proper, including costs and disbursements. See, also, Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid. regarding the 2009 action taken by The New York Times against the U.S. Government based on the FOIA with the request for the extent of law enforcement requests for social media site information. Also, Complaint against Facebook Inc. has been submitted to the U.S. Federal Trade Commission by the Electronic Privacy Information Center (EPIC), on December 17, 2009 (see the Complaint at http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf [last access, June 5, 2010]; and supplemental materials to the Complaint at http://epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf [last access, June 5, 2010]); and a second Complaint, Investigation request and Injunction and Other relief submitted to FTC on May 10, 2010, by EPIC and 14 privacy and consumer protection organizations in the U.S., i.e. The Bill of Rights Defense Committee, The Center for Digital Democracy, The Center for Financial Privacy and

Human Rights, Center for Media and Democracy, Consumer Federation of America, Consumer Task Force for Automotive Issues, Consumer Watchdog, FoolProof Financial Education, Patient Privacy Rights, Privacy Activism, Privacy Journal, The Privacy Rights Clearinghouse, The U.S. Bill of Rights Foundation, U.S. PIRG, available at http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf [last access, June 5, 2010]. EPIC's second complaint is charging that Facebook has engaged in unfair and deceptive trade practices in violation of consumer protection law. The complaint states that changes to user profile information and the disclosure of user data to third parties without consent "violate user expectations, diminish user privacy, and contradict Facebook's own representations." The complaint also cites widespread opposition from Facebook users, Senators (see April 27, 2010 letter of Senators Charles E. Schumer, Michael F. Bennet, Mark Begich, and Al Franken to Mark Zuckerberg available at http://voices.washingtonpost.com/posttech/Schumer-Franken-Bennet-Begich%20Letter%20to%20Facebook%204.27.10.pdf [last access, June 5, 2010]), bloggers, and news organizations. In a letter to Congress (see it at http://epic.org/privacy/facebook/EPIC_FB_FTC_Complaint_Letter.pdf [last access, June 5, 2010]), EPIC urged the Senate and House Committees with jurisdiction over the FTC to monitor closely the Commission's investigation. The letter noted the FTC's failure to act on several pending consumer privacy complaints.

83. On March 16, 2010, the EFF posted online documents shedding light on how U.S. law enforcement agencies use social networking sites to gather information in investigations. The records, obtained from the Internal Revenue Service and Department of Justice Criminal Division. The U.S. IRS employees are trained through a 2009 training course with the aim to use various Internet tools—including social networking sites and Google Street View—in order to investigate taxpayers. The U.S. Department of Justice Computer Crime and Intellectual Property Section were found to present detail information upon several social media companies' data retention practices and responses to law enforcement requests. Facebook was reported in said information to be "often cooperative with emergency requests" from said agencies. See more, Hofmann, M., (2010), EFF Posts Documents Detailing Law Enforcement Collection of Data From Social Media Sites, available at http://www.eff.org/deeplinks/2010/03/eff-posts-documents-detailing-law-enforcement [last access, June 5, 2010].

84. Marwick, A., Diaz, D. M., and Palfrey, J., 2010), ibid.

85. One example of secondary uses that has gained wide public attention is the practice of company personnel managers crawling user profiles of job applicants or employees: According to press reports, one third of human resources managers already admit to use data from social network services in their work, e.g. to verify and/or complete details of job applicants. See, also, related video titled Facebook Killed the Private Life, November 6, 2007, and discussion with Clay Shirky, Professor at New York University, expert on new media and social network media, available at http://www.youtube.com/watch?feature=related&hl=el&v=azIW1xjSTCo [last access, June 5, 2010].

86. Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid.; Debatin, B., Lovejoy, J., Horn, A.K., and Hughes, B., (2009), ibid.; Jones, H., and Soltren, J.H., (2005), ibid.

87. Iglezakis, I., (2010), Privacy Protection and Electronic Governance, in Protection of Privacy & Information and Communication Technologies—Technical and Legal issues, Labrinoudakis, K., Mitrou, L., Gritzalis, S., Katsikas, S., eds., Papassotiriou publications; Sotiropoulos, V., (2007), Further Use of Information in the Public Sector, Sakkoulas Publications.

88. RISEPTIS Report, (2009), Trust in the Information Society, A Report of the Advisory Board, RISEPTIS (Research and Innovation on Security, Privacy and Trustworthiness in the Information Society), available at http://www.think-trust.eu/general/news-events/riseptis-report.html [last access, June 5, 2010].

89. European Commission, (2010), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, A Digital Agenda for Europe, COM(2010) 245, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF [last access, June 5, 2010].

90. The European Data Protection Supervisor, (2010), Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, March 18, 2010, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf [last access, June 5, 2010]; European Commission, (2010), COM(2010) 245, ibid.

91. European Commission, (2010), COM(2010) 245, ibid.

92. 'Privacy by Design' is introduced as a new principle in the E.U. which is not only relevant for responsible controllers, but also for vendors and developers. It is certain that there will also be some scope for 'Privacy by Default' settings in specific areas such as RFID, social networking sites and cloud computing. See Hustinx, P., (2010), Making data protection more effective: challenges and opportunities, ICT Committee - Breakfast Roundtable: "Data Loss Prevention – Is sensitive information leaving your organization?" March 9, 2010, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-03-09_DP_more_effective_EN.pdf [last access, June 5, 2010]; the same, (2010), Recent developments in the European Union, speech given at Joint ICCP-WPISP Roundtable "30 years after: the impact of the OECD Privacy Guidelines", Paris, March 10, 2010, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-03-10_Privacy_guidelines_EN.pdf [last access, June 5, 2010].

93. Wong, R., (2009), Social Networking: a conceptual analysis of a data controller, Communications Law v.14(5) 142, available at http://works.bepress.com/cgi/viewcontent.cgi?article=1008&context=rebecca_wong [last access, June 5, 2010]; Article 29 Data Protection Working Party, Opinion 5/2009 on social networking party, WP 163/01189/09/EN, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf [last access, June 5, 2010].

94. Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169/00264/10/EN, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf [last access, June 5, 2010].

95. When Facebook users do not change privacy settings for any reason including the fact that may be unaware of the implications of not changing them or do not know how to do it, this fact of not changing the privacy settings cannot mean in consideration of data protection law in Europe that individuals have made an informed decision to accept sharing information through Facebook Platform and/or Applications which favor disclosure of personal data by default. See more at The European Data Protection Supervisor, (2010), ibid.

96. These risks have already been analyzed in the "Report and Guidance on Privacy in Social Network Services" (Rome Memorandum) of the 43rd meeting of the International Working Group on Data Protection in Telecommunications (3-4 March 2008), and in the ENISA Position Paper No.1 "Security Issues and Recommendations for Online Social Networks."
97. The European Data Protection Supervisor, (2010), ibid.
98. Facebook Privacy Policy, Risks inherent in sharing information, available at http://www.facebook.com/policy.php [last access, June 5, 2010]: "Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings."
99. Piskopani, A.M., (2010), The Facebook Phenomenon: Dismantling Privacy Protection Law, in Protection of Privacy & Information and Communication Technologies—Technical and Legal issues, Labrinoudakis, K., Mitrou, L., Gritzalis, S., Katsikas, S., eds., Papassotiriou publications.
100. Fung P., (2007), Public Search Listings on Facebook, Posting to the Facebook Blog on Sept.5, 2007, available at http://blog.facebook.com/blog.php?post=2963412130 [last access, June 5, 2010].
101. Fung P., (2007), ibid. The information that Facebook users posted through Facebook Platform and which went public was information that by default everyone could have access to. It was "Everyone" Information in the sense that information set to everyone "is publicly available information, just like your name, profile picture, and connections. Such information may, for example, be accessed by everyone on the Internet (including people not logged into Facebook), be indexed by third party search engines, and be imported, exported, distributed, and redistributed by us and others without privacy limitations. Such information may also be associated with you, including your name and profile picture, even outside of Facebook, such as on public search engines and when you visit other sites on the internet. The default privacy setting for certain types of information you post on Facebook is set to "everyone." You can review and change the default settings in your privacy settings. If you delete "everyone" content that you posted on Facebook, we will remove it from your Facebook profile, but have no control over its use outside of Facebook."
102. Abram C., (2007), Pass it on, Posting to the Facebook Blog on Dec.18, 2007, available at http://blog.facebook.com/blog.php?post=7830237130 [last access, June 5, 2010].
103. Abram C., (2007), ibid.
104. Abram C., (2007), ibid.
105. Facebook Privacy Policy states that "You can also use your privacy settings to limit which of your information is available to 'everyone'". Thus, the 'everyone' becomes the default for information posted in Facebook Platform by its users.
106. The Facebook principles is now expressed through the Facebook Privacy Policy text that is available at http://www.facebook.com/policy.php [last access, June 5, 2010].
107. Hashemi Y., (2009), ibid. The same meaning is now expressed in rephrase through the Facebook Privacy Policy in the Risks inherent in sharing information, which states that "Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that

only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook. You can reduce these risks by using common sense security practices such as choosing a strong password, using different passwords for different services, and using up to date antivirus software."

108. Facebook Privacy Policy, Risks inherent in sharing information, available at http://www.facebook.com/policy.php [last access, June 5, 2010].

109. Facebook Privacy Policy reminds—among other issues –to its users that when they post information on another user's profile or comment on another user's post, that information will be subject to the other user's privacy settings. If they use an external source to publish information to Facebook (such as a mobile application or a Connect site), they should check the privacy setting for that post, as it is set by that external source.

110. Facebook announced its intention to keep copies of users' messages online, even after they had left the network. But this decision was met with severe Facebook users' protests, and Facebook was forced to retreat from implementing this plan. See, Johnson B., and Hirsch A., (2009), Facebook backtracks after online privacy protests, available at http://www.guardian.co.uk/technology/2009/feb/19/facebook-personal-data [last access, June 5, 2010].

111. Elkins S., (2007), A Social Network's Faux Pas?, Newsweek, available at http://www.newsweek.com/id/69275 [last access, June 5, 2010]. See also Facebook groups titled "Petition: Facebook, stop invading my privacy" available at http://www.facebook.com/group.php?gid=5930262681 [last access, June 5, 2010] that counts more than 72,000 members; and "Millions Against Facebook's Privacy Policies and Layout Redesign" available at http://www.facebook.com/group.php?gid=27233634858 [last access, June 5, 2010] that counts more than 2,273,000 members; and "News feed Was the Least of our Worries—People Against an Open Facebook" available at http://www.facebook.com/group.php?gid=2210053630 [last access, June 5, 2010].

112. Hashemi Y., (2009), ibid., describes very low response from Facebook users to relevant Facebook groups protesting about public search listings.

113. McGeveran, W., (2007), Facebook Inserting Users Into Ads, post in Info/Law Blog available at http://blogs.law.harvard.edu/infolaw/2007/11/08/facebook-social-ads [last access, June 5, 2010].

114. McCarthy, C., (2007), Legally, Are Facebook Social Ads Kosher?, C|Net News, available at http://news.cnet.com/8301-13577_3-9817421-36.html [last access, June 5, 2010].

115. Felt, A., and Evans, D., (2008), Privacy Protection for Social Networking APIs, available at http://www.eecs.berkeley.edu/~afelt/privacybyproxy.pdf [last access, June 5, 2010]; Felt, A., (2007), Defacing Facebook: A Security Case Study, available at http://www.eecs.berkeley.edu/~afelt/facebook-xss.pdf [last access, June 5, 2010].

116. Facebook Privacy Policy includes clauses regarding information sharing and third parties in which Facebook states that "We do not own or operate the applications or websites that you use through Facebook Platform (such as games and utilities). Whenever you connect with a Platform application or website, we will receive information from them, including information about actions you take. In some cases, in order to personalize the process of

connecting, we may receive a limited amount of information even before you connect with the application or website." Facebook also warns a user that "You should always review the policies of third party applications and websites to make sure you are comfortable with the ways in which they use information you share with them. We do not guarantee that they will follow our rules. If you find an application or website that violates our rules, you should report the violation to us on this help page and we will take action as necessary."

117. Piskopani, A.M., (2009), Privacy Protection for Facebook users, DiMEE magazine, 3/2009, v.23, 338-353; the same, (2010), ibid.

118. Facebook Privacy Policy, Information You Share with Third parties also states that "When you connect with an application or website it will have access to General Information about you. The term General Information includes your and your friends' names, profile pictures, gender, user IDs, connections, and any content shared using the Everyone privacy setting. We may also make information about the location of your computer or access device and your age available to applications and websites in order to help them implement appropriate security measures and control the distribution of age-appropriate content. If the application or website wants to access any other data, it will have to ask for your permission."

119. Hull G., Lipford H. R., Latulipe C., (2009), Contextual Gaps: Privacy Issues on Facebook.

120. Hull G., Lipford H. R., Latulipe C., (2009), ibid.

121. In a recent experiment, antivirus company Sophos created a profile page for 'Freddi Staur' (an anagram of 'ID Fraudster'), a green plastic frog with only minimal personal information in his profile. They then sent out 200 friend requests to see how many people would respond, and how much personal information could be gleaned from the respondents. The following are some of the results: a) 87 of the 200 users contacted responded to Freddi, with 82 leaking personal information (41% of those approached); b) 72% of respondents divulged one or more email address; c) 84% of respondents listed their full date of birth. See more Sophos, (2007), Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves, available at www.sophos.com/pressoffice/news/articles/2007/08/facebook.html [last access, June 5, 2010].

122. Google's cache and the Internet Archive's Wayback Machine can be used with the aim to retrieve the online tracks which people leave.

123. Hull G., Lipford H. R., Latulipe C., (2009), ibid. And even when she deletes them, it cannot be taken for granted that the deleted content is not traceable and visible at all.

124. Hull G., Lipford H. R., Latulipe C., (2009), ibid.

125. Pearlman, L., (2007), Facebook Ads, Posting to the Facebook Blog on Nov.7, 2007, available at http://blog.facebook.com/blog.php?post=6972252130 [last access, June 5, 2010].

126. Facebook Privacy Policy describes social advertising through Facebook Platform as a pairing of relevant information that Facebook has about the user and her friends' behavior through the Platform with the aim to make advertisements more interesting and more tailored to the user and her friends. For example, Facebook states that if a user connects with her favorite band's page, Facebook may display her name and profile photo next to an advertisement for that page that is displayed to her friends.

127. In Facebook Privacy Policy, Facebook states that they share the personally identifiable information visible in the social ad only with the user's friend who can see the ad. Users can opt out of having their information used in social ads.

128. Hashemi Y., (2009), ibid.

129. Traditionally the number of visitors of a website is used as a measure of this website's success. Conversion tracking is a process to find out how many of these visitors perform actions on this website that the website operators and/or right-holders want them to perform. Any marketing campaign is pretty useless if it generates many visitors of a website but none of these visitors is "converted" into a customer. Converting visitors to customers is what most of todays commercial websites are about. Conversion Tracking is a form of website traffic analytics that measures the effectiveness of a source directing visitors to a website and persuading them to take a desired action. The source could be a referrer, a search engine, a search phrase used etc. It could also be a characteristic of the visitor for instance the country, age, income, or any other data—including personal or sensitive data—about the data subject. The desired action could be the completion of an order page, the sign-up of a newsletter, service etc offered in or through the commercial website. The effectiveness is expressed as a percentage called the "conversion rate."

130. There are many conversion tracking methods such as the Log Analysis method according to which the log files generated by the web server on which a website resides are analyzed. Conversion tracking reports are generated which are used for analysis. There is also the Tracking Services method according to which tracking script is inserted into pages of the website to be tracked. Page requests from visitors triggers the tracking script which updates some kind of a database at the tracking service. Authorized personnel log into the tracking service and generate reports which are used for analysis. There are other methods for conversion tracking, too.

131. Facebook does not provide any clarifications or examples upon the non-personally identifiable attributes of its users. It does not, also, provide any clarifications upon the anonymization process that the company follows with the aim to covert personal and sensitive data to non-personally identifiable attributes.

132. Facebook Privacy Policy, To serve personalized advertising to you, states that "We don't share your information with advertisers without your consent. (An example of consent would be if you asked us to provide your shipping address to an advertiser to receive a free sample.) We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show to other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements."

133. Hotaling, A., (2008), Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting, CommLaw Conspectus, v.16 (2008), 529-565, available at http://commlaw.cua.edu/res/docs/11_Hotaling.pdf [last access, June 5, 2010].

134. See video titled Mike Arrington interrogates Mark Zuckerberg, Upstream Recorded Live, January 8, 2010, available at http://www.ustream.tv/recorded/3848950 [last access, June 5, 2010].

135. Fletcher, D., (2010) ibid., Time magazine, May 31, 2010.

136. Kirkpatrick, M., (2009), Zuckerberg Changes His Own Privacy Settings, December 11, 2009, available at http://www.readwriteweb.com/archives/zuckerberg_changes_his_own_privacy_settings.php [last access, June 5, 2010]; the same, (2009), Why Facebook Changed its Privacy Strategy, December 10, 2009, available at http://www.readwriteweb.com/archives/why_facebook_changed_privacy_policies.php [last access, June 5, 2010]. See, also, video titled 60 Minutes—Facebook, January 14, 2008, available at http://www.youtube.com/watch?v=1UNrqz6X-AE&feature=related [last access, June 5, 2010].

137. Kirkpatrick, M., (2010), Mark Zuckerberg on Data Portability: An Interview, ReadWriteWeb, March 10, 2010, available at http://www.readwriteweb.com/archives/mark_zuckerberg_on_data_portab.php [last access, June 5, 2010].

138. Trevelyan, L., (2009), Facebook answers critics on privacy, video BBC News, February 27, 2009, available at http://news.bbc.co.uk/2/hi/business/7916137.stm [last access, June 5, 2010].

139. See, for example, Facebook's retreat regarding the use of people's picture and profile information, in Higham, N., (2009), Facebook 'withdraws' data changes, video BBC News, February 18, 2009, available at http://news.bbc.co.uk/2/hi/science/nature/7897172.stm [last access, June 5, 2010].

140. See, for example, Denham, E., (2009), Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act, available at http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf [last access, June 5, 2010].

141. Such as ENISA, Article 29 Data Protection Working Party, European Data Protection Supervisor, to name a few.

142. The European Commission has entered into an agreement with twenty social network providers known as the "Safer Social Networking Principles for the EU," available at http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf [last access, June 5, 2010]. See, also, Report on the assessment of the implementation of the Safer Social Network Principles for the EU, available at: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf [last access, June 5, 2010]. See, also, International Working Group on Data Protection in Telecommunications, (2008), Report and Guidance on Privacy in Social Network Services—Rome Memorandum, 43rd meeting, 675.36.5.

143. Liu, J., (2010), Facebook privacy settings 'unacceptable', video BBC News, May 13, 2010, available at http://news.bbc.co.uk/2/hi/business/8681781.stm [last access, June 5, 2010].

144. Indicatively cited news coverage on Facebook and privacy: IN.GR, (2010), Quit Facebook Day—After Facebook, what?, May 25, 2010; see, also, site titled We Are Quitting Facebook, May 31, 2010, available at http://www.quitfacebookday.com [last access, June 5, 2010], which has been created by Facebook users who protest against the company's alleged lack of respect for users' personal data. By May 31, 2010, the Facebook Quitters leaving Facebook via said site counted to more than 34,000 users; TA NEA, (2010), Facebook under siege, May 22, 2010; TO VIMA, (2010), Protesting for data use -- Disenchanted users organize campaign to sign out Facebook, May 23, 2010; KATHIMERINI, (2010), Facebook: Firings from U.S.A. and E.U. regarding personal data, May 13, 2010; KATHIMERINI, (2010), Front Against Facebook in Germany because

of Personal Data, April 7, 2010; TA NEA, (2010), Facebook gave out Instant Messages of its users, May 6, 2010; Helft, M., (2010), Facebook Bows to Pressure Over Privacy, New York Times, May 26, 2010; Worthen, B., (2010), Facebook Redesigns Privacy Controls, Wall Street Journal, May 27, 2010; Wortham, J., (2010), Facebook retools privacy control—Simplified settings unveiled in response to outcry over accessibility of data, Boston Globe, May 27, 2010; Liedtke, M., (2010), Senators see privacy problem in Facebook expansion, Boston Globe, April 27, 2010; Perez, S., (2009), How Facebook's New Privacy Changes Will Affect You, ReadWriteWeb, December 2, 2009; Kirkpatrick, M., (2010), The Facebook Privacy debate: What You Need to Know, ReadWriteWeb, January 18, 2010; Kirkpatrick, M., (2009), The Day Has Come: Facebook Pushes People to Go Public, ReadWriteWeb, December 9, 2009, available at http://www.readwriteweb.com/archives/facebook_pushes_people_to_go_public.php [last access, June 5, 2010]; the same, (2009), Facebook Wants You to Be Less Private—But Why?, ReadWriteWeb, July 1, 2009; the same, (2009), A Closer Look at Facebook's New Privacy Options, ReadWriteWeb, June 29, 2009, available at http://www.readwriteweb.com/archives/a_closer_look_at_facebooks_new_privacy_options.php [last access, June 5, 2010]; Singel, R., (2007), Private Facebook Pages are not so Private, Wired magazine, available at http://www.wired.com/software/webservices/news/2007/06/facebookprivacysearch [last access, June 5, 2010]; Carole, M., (2006), Privacy Fears Shock Facebook, Wired magazine, available at http://www.wired.com/science/discoveries/news/2006/09/71739 [last access, June 5, 2010]; Bruce, C., (2007), CIA gets in Your Face(book), Wired magazine, available at http://www.wired.com/techbiz/it/news/2007/01/72545 [last access, June 5, 2010]. See, also, related video posted online and titled The Truth about Facebook!, September 6, 2007, available at http://www.youtube.com/watch?v=B37wW9CGWyY [last access, June 5, 2010]. See, also, sarcastic video on Facebook, titled FaceBook in Reality—idiotsofants.com and BBC's The Wall, April 28, 2008, available at http://www.youtube.com/watch?v=nrlSkU0TFLs&NR=1 [last access, June 5, 2010].

145. Facebook Inc., plans to go for an I.P.O. See more, Vascellaro, J., (2010), Investors Bet on Price of Facebook IPO, Wall Street Journal, March 4, 2010, available at http://blogs.wsj.com/digits/2010/03/04/investors-bet-on-price-of-facebook-ipo [last access, June 5, 2010].

146. RISEPTIS Report, (2009), ibid.

147. ENISA Position Paper No.1, (2007), ibid.

148. There is disagreement about it. There are those who support that rather than rushing to generate industry compliance with "soft law" which mandates software defaults, or even considering legislation of a more traditional variety, we should be doing nothing at all. See, for example, Edwards, L., and Brown, I., (2009), Data Control and Social Networking: Irreconcilable Ideas?, Harboring Data: Information Security, Law and the Corporation, A. Matwyshyn, ed., Stanford University Press, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1148732 [last access, June 5, 2010].

149. Vice-President of the European Commission and Commissioner Viviane Reding has already started negotiations between the E.U. and the U.S. aiming at reaching deal between the two parties regarding founding principles for privacy protection and data subjects' right. The European Commission adopted a mandate to negotiate a new personal data protection agreement with the U.S. It will be the first time that the E.U. and the U.S. negotiate together high data protection standards for their citizens whenever

data is transferred and processed to fight crime and terrorism. See related video titled Commissioner Reding presents plan for EU-US data protection deal, May 26, 2010, available at http://ec.europa.eu/avservices/video/video_prod_en.cfm?type=details&prodid=14252 [last access, June 5, 2010]. The European Parliament, in a resolution on March 26, 2009, called for an E.U & U.S. agreement that ensures adequate protection of civil liberties and personal data protection. See Resolution 2010/C 117 E/32 of the European Parliament available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:117E:0198:0206:EN:PDF [last access, June 5, 2010]. In December 2009, the European Council invited the Commission to propose a Recommendation "for the negotiation of a data protection and, where necessary, data sharing agreements for law enforcement purposes with the US." See Council of the European Union, 17024/09, The Stockholm Programme—An open and secure Europe serving and protecting the citizens, available at http://www.se2009.eu/polopoly_fs/1.26419!menu/standard/file/Klar_Stockholmsprogram.pdf [last access, June 5, 2010].

150. European Commission, (2010), ibid., COM(2010) 245, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF [last access, June 5, 2010].

# Copyright exceptions and limitations for persons with print disabilities: the innovative Greek legal framework against the background of the international and European developments

**Maria-Daphne Papadopoulou**

## Introduction

At a time when sighted people are swamped with information and enjoy unprecedented ease of access to copyright protected content, a combination of economic, technological and legal factors, including the operation of copyright systems are converging to impede access to this content by the blind or other print disabled people.

According to the World Health Organization (WHO) about 314 million people are visually impaired worldwide, 45 million of which are blind (Visual impairment and blindness, 2009). Studies in the UK (Visual impairment and blindness, 2009) indicate that only 5% of books are made available within one year of publication in a format accessible to visually impaired people (such as a Braille, large print or audio-formats - Friend, 2009). 47% of blind and partially-sighted students in higher education are unable to obtain needed textbooks in their preferred formats and 33% of visually impaired children have problems accessing school books in an accessible format. This leads to a book famine phenomenon depriving people of access to education, culture and entertainment.

### *Beneficiaries*

It is important to clarify at the outset the beneficiaries, in favour of who the exception has been introduced. Even in the framework of Standing Committee on Copyright and Related Rights (SCCR) different terms have being used regarding the description of beneficiaries: 'visually impaired persons' (Sullivan, 2006), 'reading disabled' (Conclusions of the 17th SCCR, 2008), 'persons with visual or hearing impairments' and 'persons with other sensory disabilities' (SCCR/18/2, 2009), 'visually impaired and other reading disabled' and 'visually impaired and persons with other disabilities' (Conclusions of the 18th SCCR, 2009) and finally 'persons with print disabilities' (Conclusions of the 19th SCCR, 2009).

Which one is the most appropriate term referring to problems of access to published written works? The term 'visually impaired', 'reading disabled', 'print disabled' or something else?

The term 'visually impaired persons' (or VIPs) refers to blind or partially sighted people. The term 'print disabilities' covers a wide range of issues beyond visual disabilities. However, the large majority of people regarded as having a print disability are included in this category because of greater or lesser degree of visual impairment (Dakin and Wijesena, 2005, Annex II of IGC, 1985). Reading or print disabled people are all those who due to an impairment that may be physical, sensory or other, cannot read standard print. For instance, a person without sight, a person whose sight is severely impaired, a person unable to focus or move his/her eyes. It also applies to those who have a perceptual or cognitive disability which prevents them from reading standard print. Nevertheless, the term does not apply to all disabled people. For instance, a wheelchair user who has no impairment preventing him or her from reading standard print is not a 'print disabled' (SCCR/19/13/Corr., Friend 2009).

Nationally, various definitions of the visually impaired exist, some of them are inclusive in terms of the disabilities covered by copyright exceptions (e.g. the United Kingdom, Visually Impaired Persons, Act 2002 and Denmark, Section 17 of the Danish Copyright Act of 2003) others merely descriptive (e.g. USA, the Chafee Amendment to Chapter 1 of title 17, United States Code, section 121 and EU, Directive 2001/29/EC, Article 5 (3)(b) refers to "**people with a disability**").

Internationally, different approaches have been expressed. In the Proposal for a WIPO Treaty for Improved Access for Blind, Visually Impaired and other Reading Disabled Persons (SCCR/18/5, 2009) the following language is proposed for the issue in question:

"Article 15. Disabilities Covered

(a) For the purposes of this Treaty, a 'visually impaired' person is:
1. a person who is blind; or
2. a person who has a visual impairment which cannot be improved by the use of corrective lenses to give visual function substantially equivalent to that of a person who has no visual impairment and so is unable to access any copyright work to substantially the same degree as a person without a disability.
(b) Contracting Parties shall extend the provisions of this Treaty to persons with any other disability who, due to that disability, need an accessible format of a type that could be made under Article 4 in order to access a copyright work to substantially the same degree as a person without a disability".

In the last Draft proposal of the USA for a consensus instrument to WIPO during the open-ended consultations in May 2010 the term "persons with print disabilities" is used and its definition includes the following: "a) a person who is blind,

or b) a person who has a visual impairment or a perceptual or reading disability which cannot be improved by the use of corrective lenses to give visual function substantially equivalent to that of a person who has no such impairment or disability and so is unable to read printed works to substantially the same degree as a person without an impairment or disability, c) a person who has an orthopedic- or neuromuscular-based physical disability that prohibits manipulation and use of standard print materials".

'Reading' is also defined pursuant to WHO's International Classification of Functioning, Disability and Health (ICF). According to ICF 'reading' (class d 166) is defined as: "Performing activities involved in the comprehension and interpretation of written language (e.g. books, instructions or newspapers in text or Braille), for the purpose of obtaining general knowledge or specific information."

In the European Proposal also the term 'person with a print disability' is adopted and it means any person:

"a) who is blind; or
b) who has an impairment of visual function which cannot be improved, by the use of corrective lenses, to a level that would normally be acceptable for reading without a special level or kind of light; or
c) who is dyslexic; or
d) who is unable, through physical disability, to hold or manipulate a book; or
e) who is unable, through physical disability, to focus or move his eyes to the extent that would normally be acceptable for reading; and whose disability results in an inability to read commercially available standard editions of works; and who can be helped to read by reformatting the content (but, does not require the text itself to be re-written in simpler terms to facilitate comprehension)."

The choice of the beneficiaries' definition is clearly not only a legal but also a political choice. In the national legislations, where an exception in favour of the print disabled is provided, in most cases the issue has been solved. In the international forum the question has to be answered in the case of the establishment of a legal instrument and kind of the answer is crucial, since it will designate the beneficiaries.

The best approach seems to be a language consistent with the recommendations by Sullivan expressed in the "Study on copyright limitations and exceptions for the visually impaired" prepared for WIPO: "The best way to define the end beneficiary is likely to be by using a functional definition. A functional definition would be based on a person's inability to read the material that has already been published" (2006).

For the needs of the present paper we will mainly use the term 'print disabled', since on the one hand it seems to gain ground lately in the international fora and on the other hand it covers a wide range of issues beyond visual disabilities.

## Copyright implications

One of the most important problems of the print disabled is their inability to read a printed document, i.e. the access to information and consequently to knowledge. According to national constitutional rights and -most importantly- according to the UN Convention on the Rights of Persons with Disabilities (especially relevant are the Articles 4, 9, 21 and 30), these persons do enjoy a right for equal access to information products, publications and cultural material in accessible formats. Nevertheless, equal access to knowledge and information presupposes that the information is technically accessible and that there are no legal obstacles for this access (no mention is made to the economic barriers to access the information, because this analysis goes beyond the needs of this paper). From a technical point of view, several possibilities have been developed during the last decades so that these works are accessible by the persons with print disabilities. Works have to be adapted in some way, including enlarging, altering features such as color or font, transferring into a tactile code or into an audio format. The result may be hard copy Braille, large print, tape or CD, or it may take the form of temporary output from computer peripherals, such as synthetic speech or enlarged screen display (e.g. Moon, Daisy, talking books) (Garnett, 2006, Bergman-Tahon, 2009).

From a legal point of view the making of an accessible copy of a work in traditional formats or with advanced access technologies involves making both a reproduction and an adaptation of the original work. The different distribution methods for giving accessible copies to the print disabled either as physical copies or by electronic delivery online could implicate acts controlled by the rights of distribution and communication to the public. All these acts, the reproduction, adaptation, distribution and communication to the public, are restricted by copyright, since they belong to the exclusive economic rights of the rightholder and his permission must be acquired in advance, in the case of usage of a copyright protected work. Generally, any use of the work requires copyright clearance, unless it falls within the scope of an exception. Without copyright clearance and without the existence of an exception, print disabled persons encounter insurmountable obstacles accessing works and consequently receiving information.

Some national legislation do provide exceptions in favour of print disabled and these exceptions cover a range of restricted acts and protected material. A survey published by the World Intellectual Property Organization (WIPO) in 2006

showed that the copyright laws of 57 countries (out of 184 WIPO member states) contain specific provisions to assist visually impaired people, or people with other print disabilities (Sullivan, 2006; SCCR/19/3, 2009).

Nevertheless, no provision exists in any international treaty or convention concerning specifically copyright, which provides for exceptions in favour of the print disabled (Sullivan, 2006). A number of international agreements address merely the need for solutions to the difficulties encountered by print disabled, such as the Universal Declaration of Human Rights (UDHR), especially Articles 19 and 27,[1] the General Assembly of Standard Rules on the Equalization of Opportunities Persons with Disabilities (Rule 5)[2] and the Convention on the Rights of Persons with Disabilities (Articles 9, 21, 30 and 32)[3]. Some of those instruments require countries to take the needs of print disabled into account when framing their copyright laws (Article 30(3) Convention on the Rights of Persons with Disabilities).

The first supranational instrument, where an exception to the benefit of the print disabled is regulated, is European Directive 2001/29/EC [hereinafter Information Society Directive) (Article 5(3)(b)]. The Directive stipulates that all Member States shall adopt necessary measures which will facilitate access to works by persons suffering from a disability that constitutes an impediment to use of the works, and to pay particular attention to accessible formats (Preamble 43). The Information Society Directive permits exceptions to the reproduction, communication to the public and distribution rights[4] for the benefit of people with a disability subject to certain conditions and under the condition that it is complied with the three-step-test.

The situation already described can be characterized as the basic copyright problem of getting access to copyrighted works by print disabled. Part of this problem is that nowadays by the beneficiaries request access to publishers' electronic files, which can greatly facilitate the production of accessible formats (i.e. Dedicon in Netherlands, where Dedicon that has been producing alternative format material under an agreement with the Federation of Dutch Publishers (NUV) is able to request a digital file from publishers, and of course the Greek case-see following text). However, these files are what the International Publishers Association has described as the publishers' "Crown Jewels" (Sullivan, 2006) and the rightholders believe that appropriate protection against piracy and misuse needs to be guaranteed, when it concerns the online delivery of digital formats, which can be easily reproduced and instantly disseminated over the internet. Any exchange of those files could be possible with effective security measures to protect rightholders' interests.

### *Cross-border access to the accessible copyrighted works*

These copyright problems that the print disabled have to confront in order to access copyrighted works are limited to national boundaries. The relevant copyright problems though also have an international nature, such as the problem of national boundaries around accessible copies or otherwise the cross-border access to accessible content. This is basically the reason why international fora, such as WIPO and UNESCO are dealing recently intensively with the subject.

How the individual provisions on exceptions for the benefit of print disabled that have been found in national copyright laws might work when accessible copies move between different countries is a very important matter for print disabled and those organizations assisting them (Sullivan, 2006).

The problem has not only legal implications but also economic and pragmatic ones. The ability to move accessible copies between jurisdictions would allow the costs of making accessible copies to be reduced. The effort and cost of making a master copy would not have to be repeated in each country where that accessible copy is needed. The expense per accessible copy made will be less where a large number of copies are made (economies of scale). This would in turn enable the number of titles available in accessible formats to be increased as the limited resources that can be devoted to this activity would not be wasted in unnecessary and repetitive work (SCCR/19/13/Corr. 2009).

For example, there collections in the USA, Canada, the UK, Australia and New Zealand and literally millions of print disabled readers in the 60 other countries, (where English is either spoken as the first or second choice language), could benefit from having access to these collections (Friend, 2009a).

It is evident that it would be more than useful to export and import accessible copies over borders, but there may be less agreement about what, if anything, needs to –and could- be done to facilitate this in the legal framework (Sullivan, 2006; SCCR/19/3/2009).

Despite the fact that there are a number of international treaties and conventions governing the framework for national copyright laws, the underlying premise is that copyright legislation is territorial in nature. This means that each national law may generally only make provision for the precise form of rights that exist in that territory and any exceptions to those rights only determines what activity can be undertaken in that territory without infringing copyright (Sullivan, 2006). Due to the absence of international agreements, someone who has made an accessible copy of an item in one country may not be entitled to provide a copy to somebody in another country (Dakin and Wijesena, 2005). Where activity is

undertaken across jurisdictions, there will usually be a need to consider the law of both jurisdictions and decide which law to apply to which part of the activity according to the rules of private international law.

The dilemma of applicable law in cross-border copyright disputes comes to solve a specific rule -closely associated with the principle of territoriality- the lex locis protectionis, i.e. the principle of the protecting country. The principle of the protecting country, first established in the Berne Convention [Article 5(2)], means that the law of each country for which protection is claimed applies. International copyright disputes raise intricate problems related to the effect of IP rights. Effects are understood as the scope, limitation and exceptions as well as duration of copyright. The law of the protecting country would usually apply to determine the question of limitations of rights and the question of exhaustion of rights (Toshiyuki and Paulius, 2010). Restrictions placed on the exclusive right modify the content of the latter. So, if all issues concerning the content of the exclusive right must be governed by the principle of the protecting country, exceptions and limitations to the rights granted belong to the same category. The same exceptions could play a role as defenses against copyright infringement (Torremans, 2009).

Within the European Union Rome I and Rome II Regulations cover private international law issues also with regard to IP. The prevailing approach though is that such IP related questions as existence, content, duration are not governed by the Rome II Regulation (law applicable on non-contractual obligations). These issues will have to be determined according to the choice of law provisions of the forum country. Rome II Regulation introduced a special regime only for non-contractual obligations arising from an infringement of IP rights. Rome II Regulation preserves the lex locis protectionis principle according to which "non contractual obligations arising out of infringements of IP rights are governed by the law of the country for which protection is claimed" (Article 8(1)). Additionally, parties are not allowed to make a choice of law agreement under the Rome II Regulation [Art icle 8(3) and Article (13)] (Toshiyuki and Paulius, 2010).

From this short analysis it becomes evident that, since national laws differ, the protection afforded to the rightholder is country-specific. Choice of laws arises because laws of different countries might provide different rights or right with different scope. No equal protection could be afforded, since the existence and the conditions of the exceptions in favour of disabled people vary across the nations. For this reason, a solution is sought and must be found in the international forefront.

In order to realize the complexity of this copyright problem and to comprehend the number of the exclusive rights that are implicated in the situation of inter-

national exchange of accessible copies we have to analyze a concrete example. Imagine that in country A there is a need to create an accessible format of one work for the needs of one print disabled person X. First of all it has to be checked, whether an exception exists and what its application conditions are. Assuming all the necessary conditions are met, it is allowed to proceed to the creation of an accessible copy. Depending again on the exception's regulation it may permit only a Braille reproduction or it may be permit a digital version available online. This happens in country A. In the case where another print disabled person Y in country B, needs the same book in the same format and because he does not want to spend time and money to create another one a new, she asks to receive it from person X (instead of allowing persons with print disabilities to be trusted intermediaries, in which case other implications could arise, since there are not individuals but organizations). To export the work in Braille format, the relevant exportation right should be able to be limited, based on the exception in country A. And since the exportation right does not form usually any exclusive right of the right holder, we refer to the distribution right. This means that in country A the exception in favour of print disabled X has to cover also the distribution right. In country B it has to be examined whether an exception does exist for the same purpose and that all the necessary conditions apply. If the answer is positive, the next issue that arises is whether the importation of the accessible copy is legal.

There are some countries that limit importation both of copies made illegally and copies made without the authorisation of the right holders. The latter would seem to include copies made quite legally under an exception (Sullivan, 2006). For some countries, there could be a particular problem with an exception that is limited to reproducing works that have been 'published'. For countries that provide for an international exhaustion of the right to judge whether a copy should be published, it may not be problematic. A copy that has been published with the consent of the rightholder anywhere in the world can probably be brought into the country B perfectly legally and so the work also counts as 'published' in country B, even if the copyright owner has not published any copies in that country.

Therefore, even if a work must have been 'published' in both the exporting and importing country, so long as a work has been 'published' in the country where the accessible copy has been made (A), then it may also count as 'published' in the country into which the accessible copy is being imported (B). The approach is not the same for countries that do not provide for international exhaustion of rights, since international treaties give the possibility to the countries to decide what provision they make in this regard. Rightholders may therefore quite legally have published a work in country (A) which is not yet available to the public in country B and importation of an accessible copy of the published work from the country A to B could be illegal, if an exception in the country B only applies to

published works. Thus, what provision is appropriate regarding distribution of accessible copies made abroad, where a country does not provide for international exhaustion of rights should be considered very carefully. It would be necessary, for instance, to decide to what extent a provision in copyright law should permit accessible copies made in another country to be circulated, even on a not-for-profit basis, and even where they benefit print disabled, but where there are no copies in normal circulation within the country (Sullivan, 2006).

Another major issue is what happens, when, although the exception in question does exist in both countries A and B -to continue our previous example- and the exception covers also the right of exportation but there is an agreement between the rightholder and the publishers prohibiting the exportation, what will be the case. The problem of the contractual overiddability appears. Is it possible a contractual agreement to override the exception in favour of the print disabled? The analysis of this issue exceeds the scope of this paper but it is unquestionable that the international copyright instruments are silent regarding the relationship between contractual freedom and copyright law and it is left to national legislators.

At European level the issue is dealt in a contradictory way. Some concrete exceptions regarding computer programs (Article 9 Directive 91/250/EE) and databases (Article 15 Directive 96/9/EC) prevail contractual agreements and the contrary provisions are deemed null and void. For all the rest exceptions though exists the rule of prevalence of contract not only in online context (Article 6(4) and Recital 53 Information Society Directive) but also in analogue environment (Article 9, which provides that the Directive shall be without prejudice to the provisions concerning the law of contract). Thus, the only remedies against abusive contractual clauses are to be found in the general rules of law. There are some proposals arguing that in certain cases the public may need to be protected from the ability to alienate the possibility to benefit from copyright exceptions, based on the rationale of the exceptions. Particularly when an exception is attributable to the protection of fundamental rights, as it is in the case of the exception in favour of the print disabled since it provides them the constitutional right of access to knowledge, contractual overridability should not be possible. The only concern is that this approach is a product of interpretation and expressly formulated in a legal text (Akester 2010).

For all those reasons, any legislative provision regulating this issue should be carefully and sensitively drawn (Sullivan 2006).

The aim of allowing international access to accessible copies can be met by international negotiation and eventually agreements and in many cases will require amendment of national laws. This purpose is within the scope of the project cur-

rently under way under the auspices of WIPO (Dakin and Wijesena, 2005) towards an international binding legislative instrument.

### *Solutions instead of an international treaty*

There are though also alternative ways of providing access to copyrighted works.

The conclusion of bilateral agreements between two countries which permit the free exchange of accessible formats between those two countries could be one. Instead of bilateral, the agreements could be multilateral encompassing more than two countries. This involves a separate international instrument dealing with the international exchange of accessible formats, adopted in the framework of WIPO. Another way providing the print disabled access to copyrighted works is the introduction of the doctrine of exhaustion. The third alternative involves amending or adding a protocol to the Berne Convention or the WCT, to permit the free circulation of special media among contracting states TRIPs (Hugenholtz and Okediji, 2008).

Softer versions of the instrument could be framed as a resolution declaration guideline or model law with the endorsement of WIPO, WTO or both (USA proposed this solution of the Model Law during the 20th Session of SCCR). Examples of such soft law initiatives include the Joint Recommendation on Internet Use developed by the WIPO Standing Committee on Trademarks (SCT) and adopted by the WIPO General Assemblies and the Paris Union in 2001, and the WIPO Joint Recommendation Concerning Provisions on the Protection of Well-Known Marks. Neither is a binding instrument, but the latter clearly is evolving into an international legal standard through its incorporation by the U.S. into several bilateral agreements (Hugenholtz and Okediji, 2008). The soft law solution is the approach that both EU and USA seem to favour at framework of SCCR negotiations.

## International Developments

The international effort to address the copyright related barriers to overcoming print disabilities is not a recent story. Already back in 1982 (25-27 October) the Working Group on Access by the Visually and Auditory Handicapped to Material Reproducing Works Protected by Copyright met at UNESCO for this purpose and a report was presented in January 1983.

In December 1983, the Executive Committee of the Berne Union and the Intergovernmental Committee of the Universal Copyright Convention decided, each on its own behalf, to ask states to provide comments on the "Model Provisions Concerning the Access by Handicapped Persons to the Works Protected by Copyright," which was drawn up by the October 1982 Working Group on the subject convened jointly by UNESCO and WIPO.

In 1985, the Executive Committee for the Berne Convention and the Intergovernmental Committee of the Universal Copyright Convention published a Report on the issue of 'Problems Experienced by the Handicapped in Obtaining Access to Protected Works' as Annex II to a report of the agenda item "Copyright Problems Raised by the Access by Handicapped Persons to Protected Works". The 26 pages long Report is a concise presentation of the main issues facing the SCCR today. In its conclusions it was recommended to be established "an entirely new international instrument which would permit production of special media materials and services in member states, and the distribution of those material and services amongst member states without restriction".

In the last years the issue came with a new dynamic at the international forefront and WIPO deals intensively with it.

WIPO's top copyright negotiation forum, SCCR, is working to facilitate access of the blind, visually impaired and other reading-disabled persons to copyright-protected works. Acknowledging the special needs of visually impaired persons (VIP) the member states gave a mandate to the 17th session of the SCCR held in November 2008, to deal, without delay and with appropriate deliberation, with those needs of the blind, visually impaired, and other reading-disabled persons. This was to include analysis of limitations and exceptions and the possible establishment of a stakeholders' platform at WIPO, in order to facilitate arrangements to secure access for disabled persons to protected works. In pursuit of this mandate WIPO has structured the VIP Initiative with the objective to make available published works in accessible formats in a reasonable time frame (all the meetings and the relevant documents are online at http://www.visionip.org/stakeholders/en/documentation.html).

Based on the above mandate the Stakeholders' Platform was established. The WIPO Secretariat invited various major stakeholders representing copyright rightholders and VIP interests to participate in the meetings realized in the framework of this Stakeholders' Platform with the aim of exploring their concrete needs, concerns, and suggested approaches in order to achieve the goal of facilitating access to works in alternative formats for people with disabilities. By the time of this paper already four meetings have taken place: The first meeting took place in Geneva, on January 19, 2009, the second meeting took place in London, on April 20, 2009, the third meeting in Alexandria (Egypt), on November 3, 2009 and the fourth meeting in Geneva, on May 26, 2010. Two working subgroups were created among the stakeholders, respectively the trusted intermediaries' subgroup and the technology subgroup, to advance common understanding in both of these areas and identify practical solutions.

In those meetings of the Stakeholders' Platform a set of elements were identified which could form the focus of a WIPO-led process involving multiple public and private sector stakeholders. These included consideration of: (1) enabling legal regime (2) technological tools for the conversion of works (3) issues of formats, standards and interoperability (4) concerns relating to development and specific needs of developing countries (5) creating and disseminating information materials and training modules and (6) assessment of particular challenges posed by the digital environment. A number of studies were identified and commissioned relating to new technologies, trusted intermediaries and technical formats, which would enhance understanding of complex technical issues and contribute to development of greater trust between the print disabled community and the rightholders. The focus of the last meeting was to take stock of the work carried out by the two subgroups of the Platform and to identify further steps needed to pursue the mandated objectives.

A recognized challenge in this regard is to achieve concrete progress within a reasonable period while dealing with the technical complexities of this endeavour. The details of the work carried out in those meetings are included in three Interim Reports (SCCR/18/4, 2009, SCCR/19/10, 2009 and SCCR/20/6, 2010).

It is gratifying that during the 18th and 19th SCCR, held in May and in December 2009 respectively, the Member States, on the basis of the interim Reports have endorsed the progress made so far, approved the further proposed steps and encouraged the WIPO Secretariat to continue the work of the Platform. Greater emphasis on participation and concerns of Developing Countries, raised by a number of Member States, has been noted and will be taken on board for the future.

WIPO in the meanwhile has organized a series of other meetings dealing with the same subject. To mention some of them an international conference took place in Geneva in July 2009 (http://www.wipo.int/meetings/en/2009/vip_ge/), another meeting, hosted by WIPO in December 2009 with a number of UN specialized agencies in Geneva, concluded with agreement on the need for closer inter-agency collaboration in favour of VIP (http://www.wipo.int/pressroom/en/articles/2009/article_0055.html), a workshop focused on Improving Web Accessibility for Persons with Disabilities occurred in Geneva in February 2010 (http://www.wipo.int/meetings/en/2010/wipo_itu_wai/) and finally WIPO co-organized with the United States Copyright Office an international training course in Washington in March 2010 regarding the improved access to copyright protected content for the blind and other persons with visual or print disabilities).

VIP Initiative aims to facilitate and enhance access to copyrighted works for the blind, visually impaired and other reading-disabled persons and stresses the importance of common activities in this area. The visionip.org website (www.vi-

sionip.org) launched by WIPO is recognized as a vehicle to support this inter-agency effort and as a platform for attracting support, exchanging of views and disseminating information to all parties interested in the issue of access to information and cultural content by VIPs and other reading-disabled persons. Most recently (May 2010) an online forum to promote exchange of ideas and to build consensus on international measures to improve access to copyright-protected works in formats suitable for visually impaired persons and others with print disabilities was launched by WIPO. The Forum (www.visionip.org/forum) is designed to stimulate debate, enhance understanding, and broaden awareness of the issue.

At the same time SCCR, having agreed to address the issue of exceptions and limitations to copyright and related rights by exploring existing and proposed national laws on the subject, with a view to strengthening international understanding on exceptions and limitations, prepared a Questionnaire on Limitations and Exceptions, in which a part was dedicated on limitations and exceptions for persons with disabilities. This Questionnaire can be used as a tool for data collection to facilitate an analysis of the status of copyright limitations and exceptions in WIPO member states.

Apart from the discussions on a series of practical measures seeking to find convergence on operational matters, such as the integration of accessibility features into publishing software and on the question of the security on sharing digital master files -both of which will hopefully lead to an increase in accessible publishing of future titles- a draft treaty has also been proposed in SCCR to develop a harmonized set of international copyright exceptions for the benefit of the VIP and other persons with reading impairments. This proposal for a treaty (based on text prepared by the World Blind Union) was submitted during the 18th Session of SCCR, in May 2009, by Brazil, Ecuador, Paraguay and Mexico (SCCR/18/5, 2009, SCCR/19/13, 2009).

The limitations and the exceptions to this proposal of a Treaty would make it permissible without the authorization of the copyright owner on a non-profit basis under certain conditions to protect the interest of copyright holders to do the following:

- Make an accessible format of a work
- Supply the accessible format or copies to a VIP by any means including by non commercial lending or by electronic communications by wire or wireless means (Article 4a)
- Undertake any immediate step to achieve these objectives.

The most important feature of this proposed treaty though is that it aspires to legalize the cross-border exchange and the sharing of the legally made collections under copyright exceptions. Specifically, it permits the export to another country

of any version of the work or copies of the work that any person or organization in one country is entitled to possess or make under the treaty proposal, and the import of that version of a work or copies of the work under the provisions of the treaty proposal in the other country (Article 8).

During the 19th session of SCCR (from December 14 to 18, 2009) it has been agreed to move forward with discussions that could lead to better access to copyright-protected works by the blind, visually impaired and other reading disabled persons. The SCCR decided to accelerate the work on copyright exceptions and limitations for the benefit of persons with reading disabilities. In concluding remarks (Conclusions of the 19th SCCR, 2009), it was noted that the Committee accepted the initiation of focused, open-ended consultations in Geneva "aimed at an international consensus regarding exceptions and limitations for print-disabled persons."

In the course of those open-ended consultations in May, 2010 USA submitted a draft proposal for a consensus instrument (Draft proposal of the USA, 2010). Although several recommendations on national laws to aid the import and export of accessible books are included in this draft proposal, this movement was not accepted with great enthusiasm from the countries that have supported the treaty proposal most importantly due to the fact it is not a legally binding instrument (other reasons that the USA's proposal failed the expectations of the countries supporting the treaty proposal was that it does not create a legal obligation for countries to establish exceptions, it does not address the need to circumvent technological protection measures or contractual restrictions on needed exceptions (Kaitlin, 2010). On the other hand Brazil, Ecuador, Mexico and Paraguay proposed a concrete timetable for the adoption of a Treaty for the visually impaired, that would see its completion till the spring of 2012 (SCCR/20/9, 2010).

EU proposed a Joint Recommendation solution (SCCR/20/12, 2010) instead of supporting a binding Treaty and also the African Group proposed a language for a Treaty covering exceptions also for educational and research Institutions, libraries and archive centers (Draft WIPO Treaty on Exceptions and Limitations for the Disabled, Educational and Research Institutions, Libraries and Archive Centers) (SCCR/20/11, 2010).

## European Developments

The issue occupies a central role at the European scene and at the latest European Union copyright developments.

In the European context there exists a legal framework regulating exceptions and limitations: the Information Society Directive. The list with the exceptions prescribed in the Directive is exclusive but not mandatory (apart from one). How-

ever, the provision of Article 5(3)(b) providing for an exception in favour of disabled people is now part of the copyright law of all Member States.

Although all Member States have implemented the relevant copyright exception into their national legislation, their approach is not harmonised, so a degree of legal uncertainty still arises. Furthermore the cross-border transfer and exchange of the accessible material continues to be impeded by the territorial limitation of exception under national legislation.

As a result in July 2008 the European Commission launched a public consultation in the form of a Green Paper in the Knowledge Economy. The Green Paper focused on general issues regarding exceptions to exclusive rights and specific issues relating to exceptions and limitations most relevant for the dissemination of knowledge. Among those exceptions was also the one for the benefit of people with a disability (the rest involved exceptions for the benefit of libraries and archives, allowing dissemination of works for teaching and research purposes, orphan works and user generated content). After examining the submissions to the public consultation (almost 400 responses from publishers, collecting societies, libraries, archives, universities, researchers, companies and consumer organizations, online at http://ec.europa.eu/internal_market/copyright/copyright-infso/copyright-infso_en.htm) the Commission published a Communication on Copyright in the Knowledge Economy in October 2009. One of the priority areas that the Communication identifies is the print access for persons with disabilities. The Commission believes that the problem of accessibility could be improved at European level in a relative short time frame through goodwill and constructive discussions among stakeholders.

According to the Communication, the immediate goal is to encourage publishers to make more works in accessible formats available to disabled persons. Technological protection measures should not be an obstacle to the conversion of legally acquired works into accessible formats. Additionally, exceptions for persons with disabilities including visually impaired persons should not be able to be contractually overridden (the British Library found that out of a sample of 100 licences it entered into with electronic publishers, only two acknowledged the exceptions for visually impaired people).

One of the benefits of the public consultation was that it revealed a number of existing and effective collaborative efforts for persons with print disabilities across the EU. For instance, in Denmark, e-books or audio-books produced by the Danish Library for the Blind are equipped with a unique ID which allows control of the use and of the work and the tracing of possible infringers. In France, agreements are in place between a not-for-profit agency BrailleNet and publishers for delivery of digital copies of works which are stored on a specialised secure server accessible only

by certified organisations [Green Paper COM(2009) 466]. The Communication underlines that such efforts should be accelerated and applied across the EU.

In order that constructive discussions among stakeholders to take place, a Stakeholder Dialogue has been set up by the European Commission concerning the needs of print disabled persons. The first meeting took place in Brussels, in December, 2009 (the importance of the issue was also highlighted at a European Parliament Workshop organized in Brussels in November 2009). The forum considered the range of issues facing the visually impaired persons and possible policy responses. In that meeting publishers, representatives of the European Blind Union and European Disabled Forum, technology experts, libraries as well as people from inside the European Commission from various departments have participated (http://www.europarl.europa.eu/activities/committees/hearingsCom.do?language=EN&page=2&body=JURI). Aim of this forum is to look also at possible ways to encourage the export of a converted work to another Member State while ensuring at the same time an adequate remuneration of the rightholders for the use of their work.

The Dialogue will also tackle the technology issues of accessible formats. A considerable amount of European funding has already borne fruits in the form of projects, such as EUAIN network and PROACCESS. [5]

## The innovative Greek legal framework

Article 28A of Copyright Law 2121/1993 is the provision concerning the exception established for the benefit of blind and other disabled (Off. Gaz. A' 25/4.3.1993). Article 28A provides the following:

Article 28A: Reproduction for the Benefit of Blinds and Deaf-mute

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.

Pursuant to Article 28A the reproduction of a previously published work is allowed and constitutes a legitimate limitation of the author's right, under the condition that the work is reproduced in special formats and solely for the benefit of certain beneficiaries, for uses which are directly related to their disability and are of a non-commercial nature, to the extent required by the specific disability and provided that the concrete application terms of the Ministerial Order are complied with. It is important to highlight that according to the exception in question only the reproduction right is limited and not the right of the communication to the public

(and the distribution right), despite the fact that the Information Society Directive offered this possibility to the national legislators [Articles 2, 3, 5 (3)(b) & (4) Information Society Directive] (for instance Cyprus, Denmark, France, Hungary, Poland, Portugal and Spain did take advantage of this possibility, Westkamp, 2007). Thus, the reproduction of a work in Braille could fall under the exception according to the Greek legal framework, its online presentation, however, not.

Another concern is that the exception for people with a disability is not specifically provided in Directive 96/9/EC on the legal protection of databases (hereinafter database Directive). Although Article 6(2) Database Directive provides for other exceptions, such as teaching or scientific research, and private use reproductions, it includes no exception for print disabled. This raises the concern that the exception for people with a disability could be undermined by invoking database protection on the basis that a particular literary work is simultaneously protected as a database, since Article 2(e) Information Society Directive leaves the provisions of the Database Directive intact. As pointed out in the Commission Staff Working Paper of 19 July 2004, this situation might arise when the literary work, such as an encyclopaedia, is protected as a work and as a database at the same time (Green Paper, Copyright in the Knowledge Economy). Accordingly the same situation appears in the Greek legal framework, where a similar exception is not included in the legal protection of a database. Thus, the exception in question does not apply to databases with all the risks that this statement brings.

The national legislator considered that the application terms of this provision should be detailed and that a specific procedure should be established in order the reproduction to be allowed. To this end it is prescribed by Copyright Law that the specific terms of application of this arrangement and all the necessary details should be determined by a Ministerial Order (by the Minister of Culture). This Ministerial Order (ΥΠΠΟ/ΔΙΟΙΚ/98546/2007, Off. Gaz. Β' 2065/2007) was enacted in October 2007, with a five years delay, since the amendment of Article 28A Law 2121/1993 was enacted in 2002 (Amendment of Copyright Law with Article 81(2) Law 3057/2002).

The non-enactment of this Ministerial Order held the regulation in abeyance and amounted to a fruitless provision, since without the necessary legal instrument the beneficiaries (blind, deaf-mute and persons with other disabilities) could not take advantage of this provision.

Analyzed in the next section, the Ministerial Order provides for the competent intermediate bodies, the beneficiaries, the categories of works whose reproduction is allowed, the formats of reproduction of a work, the publishers' obligation to provide files in electronic format and finally, the terms of applications.

### *Ministerial Order ΥΠΠΟ/ΔΙΟΙΚ/98546/2007*

In the title of this paper the Greek legislative framework is described as innovative. The logical question is what characteristics attribute to the Ministerial Order this feature. There are two: the establishment of intermediate bodies and -most importantly- the publishers' obligation to deliver to the competent intermediate bodies the files of the works to be reproduced in electronic format. In order the rightholders not to fear that this obligation could cause irrevocable damage to their interests by losing the control of the reproduction of this electronic file, the Greek solution has provided the rightholders with a number of obligations. The most significant obligation is exactly this establishment of intermediate bodies, who are responsible for the reproduction of the copyrighted works. For the detevmition of the status of beneficiaries and who are liable for any copyright infringements by third parties selected for the reproduction of the copies.

At the outset it should be pointed out that this exception allows for a free use, i.e. it permits the intermediate bodies to undertake the acts restricted under copyright or related rights protection to the extent permitted without having to contact the rightholders to obtain permission and without having to pay any remuneration.

The limitation described in Article 28A –as all the limitations applicable to the economic right (a.18-28C)– apply mutatis mutandis to the related rights (Article 52 Law 2121/1993). Thus, the limitation in favour of the blind and people with other disabilities apply also for the related rights, even though no specific mention is made neither in Article 28A nor in the Ministerial Order.

The Ministerial Order is presented and analyzed thoroughly below.

### Beneficiaries

A major issue in this exception is the eligible beneficiaries. It is discussed in the international framework whether the beneficiaries should be the visually impaired persons, the print disabled, the reading disabled and so on (see Introduction). The terminology does not reflect only matters of linguistic but it covers also different categories of disabled persons. The wider the term the more beneficiaries can invoke the exception and the greater the impact for the rightholders. Article 28A refers to blind and deaf-mute persons and gives the possibility to the Ministerial Order to widen the circle of the beneficiaries "... By Ministerial Order of the Minister of Culture ... may be determined as well as the application of this provision for other categories of people with a disability". In the Ministerial Order a functional definition -and not a medical one- was chosen based on a person's inability to read the published material on definitions for inability in law

see Bottis. Beneficiaries are not only blind and deaf mute but also people with defective or reduced vision which cannot be corrected using corrective lenses to a degree that would be satisfactory for reading, and generally people that because of a disability are unable to read a printed text in a conventional way or perceive the content of a work using their physical senses (Article 3 Ministerial Order). Thus, the Ministerial Order provides a definition so wide so as to include only the people that they suffer from a reading disability.

## Competent intermediate bodies

It is already mentioned that in the Greek legal framework intermediate bodies are used in the exception. That means that the beneficiaries are not allowed to proceed themselves to the reproduction of the relevant works but they have to refer to specific intermediate bodies, which they are competent to do so, if they comply with all legal requirements regarding their nature (Article 2(1) Ministerial Order) and with the general terms of application (Articles 7 and 6(4-7) Ministerial Order). The established conditions regarding the nature of the intermediate bodies are the following:

i) they have to be non-profit organizations or associations or unions or other pertinent organizations,

ii) whose main mission is to provide specialized services related to the education and training or to the facilitation of education and training of the blind and the other beneficiaries.

Educational establishments could also be competent bodies for the needs of the Ministerial Order. Certain academic libraries are major producers of accessible material as well as having more usual library functions in giving print disabled access to this material (Sullivan, 2006; SCCR/19/3, 2009).

In case of doubt as to whether a body is eligible to proceed to reproduction as a competent intermediate body, the Hellenic Copyright Organization (HCO) makes the final decision. The HCO maintains also a list of all competent bodies (Article 2(2) Ministerial Order).

## Categories of works allowed to be reproduced

The Ministerial Order excludes only the artistic creations as a whole from the application of this exception. From the other works of literature or science all but one may be reproduced for benefit of disabled persons in order to obtain a format that they can perceive, in the case that in its existing form cannot be perceived by the beneficiaries: the source code of computer programmes (Article 4 Ministerial Order).

Necessary condition is that the work should already have been published (Article 7(1) Ministerial Order) in accordance also with the moral right of publication (it is not clarified though whether the publication must have been a lawful one).

Additionally, the exception cannot be invoked when the works are already available in the market in formats specifically designed for the needs of beneficiaries. This should not though be interpreted in the sense that once one accessible format is commercially available, all others are excluded from the exception, since there is no one format that is accessible to all disabled beneficiaries [Article 7(2) Ministerial Order].

## Allowed formats for the reproduction

The Ministerial Order does not specify the allowed formats under the exception. The works whose reproduction is allowed may take formats such as Braille, Moon, Daisy (Digital Accessible Information System -www.daisy.org- offers the benefits of regular audio books, but they include also navigation), talking books and any other method solely designed to be used by the beneficiaries and to respond to their special needs, to the extent required by the specific disability (Article 5 Ministerial Order). In this way the law specifies that the making of copies in other formats not exclusively made for the print disabled, such as large print copies that can be read by anyone or sound recordings on media that can be played in standard audio equipment are excluded from this exception.

## Advantage for the beneficiaries

The 'innovation' that the Greek regulation brings is the publishers' obligation to deliver to the competent intermediate bodies the files of the works to be reproduced in electronic format. More specifically, publishers are obliged within thirty (30) days of the receipt of the request by the competent intermediate body, to deliver to this body (not to the beneficiaries themselves) in electronic format the files of the works to be reproduced, under the condition that the work is kept in electronic format (Dakin and Wijesena, 2005).

The Greek legal framework provides for some specific requirements regarding the nature and the quantitative limits of the works covered by the specific limitation allowing reproduction. Works that may be delivered in electronic file include all educational books of primary and secondary education and all the mandatory books of tertiary education. For all other works, the publishers shall, if so requested, deliver to the competent body electronic files of works totaling up to 10% of their annual publishing production; such percentage does not include any educational books published. In the event that the publisher refuses to comply with this obligation, the percentage doubles [Article 6(1-2) Ministerial Order].

For the system to be effective two databases should be established and kept by the HCO and the Association of Book Publishers (for the time being only the one in HCO operates, http://web.opi.gr/opifiles/tyfloi/db_tyfloi.pdf). One database includes all the intermediate competent bodies, and the second the titles of works in electronic format held by each body, the name of the author, the publisher, the ISBN and the special format in which documents have been reproduced (Article 6(6) Ministerial Order). Both of them form a useful tool and function as an information resource for the intermediate bodies and the beneficiaries when they search for works that are already reproduced in an accessible format, so as to reduce costs and time for a second unnecessary reproduction.

One additional element that must be highlighted is that the application of Ministerial Order's provisions cannot be eliminated by contract between the publisher and the author (Article 7(5) Ministerial Order). The law considered that mostly publishers would have an interest in overriding this exception and articulated in this specific way the non-overridability of the provision. However, a more general prohibition would be more appropriate, like in Germany, where there is a provision which stipulates that contracts are void if they would have the effect of overriding exceptions to copyright and in Portugal, where contractual conditions that override the exception are null and void. For traditionally published works it is highly unlikely a binding contract to be agreed between the rightholder and the potential user, which would have the effect of overriding an exception. Such contract seems more likely in online available works, more commonly in a database, accessible only by users who agree to comply with contractual terms (Sullivan, 2006).

## Obligations of rightholders' security

It is more than complicated to provide digital masters files without the necessary guarantees and safeguards for rightholders, who have to be confident that any digital format is being delivered through secure gateways only to the people who are intended to receive it. The fear of piracy and the evident ease with which it happens in the digital world are understandably a reason why there is a need to ensure that the process is carried out and maintained within a secure network and by trusted bodies. In the modern environment driven by the internet for content dissemination, security is a vital issue for rightholders (Bergman-Tahon, 2009).

The Greek legal instrument provides with a number of obligations to the security of the rightholders without though describing in detail the ways and the necessary technical measures in order the desired protection to be accomplished. Among those measures, the most important is that the restriction of the limitation applies only to the reproduction right and not to the making available right. This restriction actually constitutes the most effective measure, since it contrib-

utes to the maintenance of the strictest control to impede one literary text available in digital form, to become the source of illegally produced and distributed copies in internet (Garnett, 2006). Another measure is the establishment of the intermediate bodies being responsible for the reproductions of the works in the accessible formats. To this aim the Ministerial Order introduces specific obligations to the intermediate competent bodies, one of which is their responsibility to investigate the capacity of beneficiaries [Article 7(7) Ministerial Order]. Additionally, the intermediate competent bodies incur the principal's liability for any copyright infringements by third parties selected for the reproduction of their copies [Article 7(8) Ministerial Order].

The intermediate bodies shall notify the HCO and the Association of Book Publishers regarding the titles of the works in electronic format held by them and the special format in which the works have been reproduced [Article 6(6) Ministerial Order] in order the relevant database to be updated (http://web.opi.gr/opifiles/tyfloi/db_tyfloi.pdf. Moreover, the intermediates are obliged to notify the publisher of the number of copies reproduced and of the form of such reproduction.

Furthermore, in the event of a change in purpose or dissolution, the competent bodies must destroy all electronic files in their possession and report that destruction to the HCO and the Association of Book Publishers (Article 6(7) Ministerial Order).

The intermediate bodies are obliged to purchase one copy of the work to be reproduced, irrespective of the number of copies to be reproduced and subject to the limitations of Article 7(6) Ministerial Order.

Connected to this issue is whether or not the moral right might be infringed due to production of accessible copies, and particularly the integrity right. The Ministerial Order repeats the moral right's protection giving specifically attention to the paternity right and the integrity right.

The copy of the work reproduced pursuant to this Ministerial Order should mention the name of the author and the publisher, as well as the date of first publication, if such information is included in the work. The physical carrier of such copy should also mention that the copy has been reproduced pursuant to article 28A Law 2121/1993 and the Ministerial Order in question and that any further reproduction in formats other than the ones allowed (Article 5 Ministerial Order) will constitute an infringement of the copyright and will incur penal and civil sanctions (65 et seq. Law 2121/1993) [Article 7(3) Ministerial Order].

The text cannot be amended or changed without the authorization of the author and the publisher, in relation to each one's rights. Such prohibition does not concern though changes relating to layout and pagination, which are dictated by the

need to convert the form of the work to serve the needs of beneficiaries. Competent bodies have to respect the author's rights in the reproduction of the work and the fulfillment of its purpose [Article 7(4) Ministerial Order].

Finally, the Ministerial Order stresses out that copies reproduced on its basis cannot be used for purposes other than those provided for in the Ministerial Order. Any person making use of such a file for purposes other than those provided for (Article 1 Ministerial Order) will be liable for penal and civil sanctions (65 et seq. of Law 2121/1993) [Article 7(6)].

Save as otherwise stipulated in Law 2121/1993, any dispute arising from the non application of the Ministerial Order is resolved according to the injunction procedure (Articles 682 et seq. Code of Civil Procedure).

## Three-step test

One additional condition -or better formulated an additional test- is the three-step test, which applies in addition to other requirements in the exception for the benefit of visually impaired persons.

Although generally it is not believed to be necessary to include the wording of this test in the legal framework, the Greek Copyright Law has incorporated verbatim the three-step test that applies to all exceptions. In addition the Greek Copyright Law describes a number of conditions to the application of this exception according to the Ministerial Order (it has been supported that when an exception has to comply with the three-step test, the law should be more flexible and should demand fewer conditions) (Sullivan, 2006). The Greek legislator chose the safest way and established a double way of protection.

The difficulty here as elsewhere is to identify conditions that are reasonable in that they do not make it too difficult to help print disabled access the written word, but they do give some reassurance to right holders (Sullivan, 2006).

### *The three-step test – the general exception*

Apart from the detailed exceptions Berne Convention provides a general one in Article 9(2), which has the form of a test for determining whether or not an unauthorised reproduction is lawful. The three-step test, as it is known, provides as follows:

"It shall be a matter for legislation in the countries of the Union to permit the reproduction of such works in certain special cases, provided that such reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author."

This Article stipulates three distinct conditions that an exception to the reproduction right must be complied with in order to be justified under national law:

1. Limitation of application to 'certain special cases';
2. The unauthorized reproduction 'does not conflict with the normal exploitation of the work'; and
3. The unauthorized reproduction 'does not unreasonably prejudice the legitimate interests of the author'.

It is a vague and general criterion that allowed countries to grant exceptions to the -then- newly enshrined reproduction right and a formulation of compromise broad enough to cover all exceptions included in the legislation of the signatory countries (Senftleben, 2004; Geiger, 2007; Geiger, 2007a).

Although this provision in the framework of the Berne Convention refers only to the reproduction right, the TRIPs Agreement and the WCT (and the WPPT for the neighbouring rights) extended the application of the three-step test to all exclusive rights, to exceptions granted under Berne Convention (because of the incorporation of the latter into TRIPs) and also to any new exceptions that member states may adopt in the future. Therefore the three-step test applies not only to the reproduction right but also to all the exceptions and consequently also to the exception in favour of print disabled.

No authoritative interpretation was given to the three-step test under Berne Convention (such an interpretation could only be given by the International Court of Justice). The only case in international context that has been heard was the IMRO case in front of the WTO Panel (US Section 110(5) Report). Despite the complexity that the interpretation of the three-step test presents, we will look shortly at the three-step test itself and afterwards we will examine how it is applied on the exception in favour of print disabled. All three-steps of the test are cumulative.

## *The three-steps of the test*

### First step: 'Certain Special Cases'

The limitations and exceptions should be confined to "certain special cases". The term 'certain' means that the 'cases' (the exceptions) should be clearly defined, known and particularized, without though being explicitly identified but guaranteeing a sufficient degree of legal certainty. 'Special' is interpreted as of a narrow scope or reach, or exceptional in quality or degree. The exception should be narrow in a quantitative as well as in a qualitative sense. An exception should be the opposite of a non-special, that is to say a normal, case (US Section 110(5) Report; Ricketson, 2003).

## Second step: "Does not conflict with the normal exploitation of the work"

Regarding the second step it is accepted that it means that there should not be a conflict between the exception and the ways in which an author might reasonably be expected to exploit his work in the normal course of events (e.g. in the case of judicial proceedings) (Ricketson, 1987). More specifically the exempted uses should not enter into economic competition with the ways that authors normally extract economic value from that right and deprive them (the authors) of significant or tangible commercial gain (US Section 110(5) Report, § 6.180). If we would accept though a solely economic approach of the second step, considering that any free use permitted under Article 9(2) would have the potential of being in conflict with a normal exploitation of the work, this would have as a consequence that the third step would never be reached. Therefore, we should include in the consideration of the second step also non-economic normative considerations, namely whether this particular kind of use is one that the copyright owner should control or not. In this way there may be uses that will not be in conflict with what should be within the normal exploitation of the work (in a normative sense) but it may not satisfy the third step (Ricketson, 2003).

Furthermore, there are also other parameters that have to be considered and in any event there has to be a case-by-case assessment by the courts. There is some uncertainty but the ultimate touchstone is that the use must be 'fair' (Ricketson, 2003).

## Third step: "Does not unreasonably prejudice the legitimate interests of the author"

It is a fact that any exception prejudices to a certain degree the author's interests. The decisive factor though is the term 'unreasonably'. Prejudice to the legitimate interests of authors could turned out to be 'unreasonable', if the exception causes, or could cause, an unreasonable loss of income to the respective rightholder taking into account also the importance of the other interest at stake, that justify the exception [US Section 110(5) Report]. The unreasonable prejudice implies the lack of proportionality. The unreasonableness of this economic harm, i.e. the prejudice, that such an exception could cause, might be countered by placing some conditions on the use of the work or even by a payment made for this use. The exception may take the form of either a free use or a legal (compulsory or statutory) license, depending essentially on the concrete circumstances (Ricketson, 2003). Although the unreasonable prejudice to the legitimate interests of the authors could be avoided by the payment of remuneration, this would not

cure a use that conflicts with the normal exploitation of the work (second step) (Ricketson, 1987).

### *Application of the three-step test on the exception for the benefit of print disabled*

It is relevant to consider whether the Greek exception for the print disabled could pass successfully the three-step test.

#### First step

Regarding the first requirement, in order the use of a work to be qualified as an exception, it should be a 'certain special case'. This means, as it is already analyzed, that the case in question should be clearly defined, known and particularized, without though being explicitly identified but satisfying a certain degree of legal certainty, narrow in quantitative as well as in a qualitative sense. This first step intends to keep the scope of the exception qualitatively and quantitatively restricted, so that it may be deemed a 'special case'. Applying this requirement to our case leads us to the necessity to define a well specified exception and to determine for this purpose the beneficiaries that could evoke this exception, to determine the allowed acts, the relevant categories of works, and the exclusive rights that would be limited.

An exception that is carefully limited to assisting print disabled by permitting only to the competent intermediate bodies (Article 2 Ministerial Order) to produce the accessible copies made under the exception and to provide them with those copies, such as the Greek regulation, does appear to be a 'special case'. In addition the provision limits the application scope of the exception to cover only non profit institutions, whose main mission is to provide specialized services related to the education and training or to the facilitation of education and training of the blind and the other beneficiaries.

In the Ministerial Order not only the intermediate body but also the end beneficiary is clearly specified by using a functional definition based on a person's inability to read the material that has already been published (Article 3 Ministerial Order).

The exception here, while restricted to specified groups of end users (beneficiaries) and institutions, could nonetheless range widely to cover all kinds of works and uses. Clear definition and limitation of exceptions is therefore necessary to establish that these are 'certain special cases' within the first step of the three-step test. To this end the Ministerial Order restricts the limitation to specific work categories (Article 4 Ministerial Order), in specific quantities of the works to be reproduced [all educational books and 10% of annual publishing production –

Article 6(2) Ministerial Order] and in specific formats (Article 5 Ministerial Order). Furthermore, it underlines that the use of those works should be made only for the purpose of the Ministerial Order and the Law 2121/1993, and any other use of the works is excluded from the exception's scope [Article 7(6) Ministerial Order].

Finally, the Greek provisions cover uses that are limited only to the reproduction right, restrict the persons and the institutions that may take advantage of the exception, and the nature of the disability is defined.

Thus, the first step of the three-step test may be deemed to be satisfied here.

## Second step

The use of a copyrighted work in this context should not be undermine the normal exploitation of the work, so as the second step to be satisfied. This reproduction of works could be considered to enter into economic competition with the ways that rightholders normally extract significant commercial economic gain.

Some types of accessible formats such as audio recordings and large print, there may be significant market opportunities to increase commercial production to provide for the expanding needs of those with failing sight, as the average age of the population increases. An exception that permitted commercial activity would therefore potentially lead to activity that directly conflicts with the publishers own production of accessible formats and/or deny the original publisher the opportunity to license commercial special editions for these groups of readers/alternative format production by others (Ricketson, 2003).

The Greek law limits activity under the exception to acts that are non-commercial. The non-commercial limitation is mentioned directly in Article 28C Law 2121/1993 and Article 1 Ministerial Order and is delivered by requiring the intermediate body that acts under the exception to be non-profit making and any charges made for accessible copies are capped by not allowing a profit to be made (the Ministerial Order provides that in the event that the cost of the reproduced copy is incurred by beneficiaries, it should not exceed the reproduction cost).

The Greek exception rules out expressly not only the commercial activity but also it does not permit a work to be used, if an accessible format is already available to print disabled people. Such a provision is of paramount importance; the publishers are encouraged -or at least are given the possibility- to produce accessible copies for all groups of readers. They are not excluded from the beginning, but they do have the possibility to enter the relevant market. The crucial question remains though how big the time frame is before they decide to enter the relevant market. Publishers could make the necessary adaptation to the work at the

production stage, so that an adapted version is created at the outset. In that case, there is no need and no room for the specific exception for the print disabled [Articles 5(3)(b) and 5(4) Information Society Directive] to apply anyway, because accessible content is already provided. The rationale for the application of that particular exception disappears and only the remaining exceptions, which do not address the specific needs of people with a disability, could apply. If this provision had not existed, then no one would buy accessible copies distributed by the publishers, since other copies would have been produced and distributed without any payment to the rightholders under this exception. This would be contrary to the three-step test in any case (Sullivan, 2006).

## Third step

Assuming that we have accepted that the second step is satisfied, the problem of the third step remains and must be also satisfied. Concerning the third step we have to deliberate under which conditions and circumstances the use is allowed, so that any prejudice caused to the rightholders' legitimate interests not to be unreasonable.

This use could have an impact on the market for sales of tangible copies and consequently could harm the primary and secondary markets of the rightholders. This statement though does not lead automatically to the exclusion of exception but to the ascertainment that it should be applied with caution in order to minimize the potential harm to rightholders' interests (so actually not to prejudice 'unreasonably' their legitimate interests). Depending upon the quantity and the nature of the works that may be reproduced, the eligible groups of users/beneficiaries, the eligible for the reproduction bodies, and whether or not the use is subject to an obligation to pay fair compensation, the third step may be satisfied (Ricketson, 2003).

This caution could be interpreted as an establishment of one further requirement. The intermediate bodies must implement some conditions and even technological measures, such as digital watermarking and encryption, to ensure that the work will not be reused beyond the allowed use and additionally that the recipients will be only the ones that are supposed to be (print disabled).

Finally, the question of unreasonable prejudice needs to be considered, and it is supported that this is an area that should be subject to pay equitable remuneration, rather than being a free use. Some countries, that do have exceptions to copyright for the benefit of print disabled, combine them with mechanisms by which rightholders can be or are paid a royalty for any accessible copies made. Greece though does not belong to one of them. Generally the exception provision that has been made is governed by the three-step test but this does not neces-

sarily require a royalty payment to accompany an exception. It may, though, be easier to argue compliance with the test in some situations where right holders receive compensation for activity under an exception. Of course, exceptions vary too in the extent of the activity possible. The scope of what is permitted under an exception could be a key factor in deciding whether or not right holders should receive a royalty. As for any exception, determining the right balance between the interests of right holders and users is difficult with no precise rules about issues such as compensation (SCCR/9/7 page 127). The traditional exception in the analogue environment might not be found to be in full compliance with the three-step test, when it comes to make available online digital copies. The online availability presents a potential of uncontrolled wide scale dissemination that may affect the market for, or the value of, the copyrighted works, as well as harm otherwise the legitimate interests of the rightholders (Lung, 2004). Since the Greek relevant exception is limited only to the reproduction right, it seems that there is no apparent problem regarding the conformity of this exception with the last step of the three-step test.

The prejudice of unremunerated free use could be unreasonable to the legitimate interests of the author not only when economic interests are damaged but also in the case of moral rights interests, for instance, if a usage distorts the work or fails to identify the author. Also in this respect, the Greek provisions are consistent with the third step, in that they do not derogate from moral rights protections (Article 7(3) and (4) Ministerial Order) (Ricketson, 2003).

## Technological protection measures and the exception in favour of print disabled

Digital technology has provided great opportunities for increasing access for people with print disabilities. Paradoxically, it has also in some respects increased the practical and legal complexity of accessing material, especially with the development and use of technological protection measures (TPMs) and Digital Rights Management (DRM). By whatever name TPMs are encoded into digital content by a variety of means (such as encryption or watermarking), so that users are incapable of accessing or using the content in a manner that the rightholder wishes to prevent. The ability to use technological protection measures to prevent unauthorized copying of their works is a further addition to rightholders' arsenal.

What is the relation though between the legal protection of technological measures and the exceptions to copyright and related rights and particularly to the exception for in favour of the print disabled?

If it is a digital version protected by TPMs, the person will need a copy without TPM in order to be able to make an accessible copy. Some countries have includ-

ed provisions in their laws, so that the exception continues to apply and Greece is one of them.

So those TPMs could hinder the beneficiaries of the exception from taking advantage of the latter, exactly due to the TPMs put on the work. A solution should be found in order to regulate the protection of TPMs without depriving users allowed uses of the copyrighted works, such as use of the works in favour of print disabled. Article 6(4) Information Society Directive aims at resolving this intersection between legal protection of TPMs and the exercise of limitations or exceptions. According to Article 6(4) member states should take voluntary measures, including agreements between themselves and other parties concerned, to ensure that the beneficiary of certain limitation provided for in national law (among those also the exception in favour of print disabled) has the means of benefiting from that limitation, to the extent necessary and that the beneficiary has legal access to the protected work or subject matter concerned. The Directive remains silent regarding the voluntary measures and it is at the right owners discretion to choose those ones (e.g. supply of a non-protected version of the work; supply of an encryption key to allow the user to circumvent the TPM; deposition of the encryption key with a third party, so that upon request the beneficiary of a limitation could obtain it; designing the TPM so, that certain lawful uses are permitted) (Guibault, et al., 2007, where you can find also examples of member states).

Article 6(4) further provides that "in absence of voluntary measures taken by rightholders … Member states shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided in national law". Once more the Directive is silent what the 'appropriate measures' taken by the member states are. Therefore member states have interpreted this provision in different ways and some have established a dispute resolution or mediation mechanism (Finland, Denmark, Estonia, Hungary and Greece), some have created an executive or administrative authority in order to prevent the abuse of such measures taken by the rightholders (France), some recourse to courts (Belgium, Germany, Spain and Ireland) and finally some others have not implemented it at all (Austria, Czech Republic and Netherlands) (First evaluation of Directive 2001/29/EC, 2007). Recital 51 of the Directive, however, stresses out that member states should take appropriate measures only in absence of "voluntary measures taken by rightholders including the conclusion and implementation of agreements between rightholders and other parties". The nature of the member states intervention could refer to "modifying an implemented TPM" or "other means" (Recital 51). It is important to underline that, although the provision does create an obligation for rightholders and member states to provide the means to exercise the limitation, it does not allow beneficiaries to circumvent TPMs. Its aim is to facilitate the exercise of an exception (Den-

mark and Norway have entitled though beneficiaries to circumvent TPMs under certain narrow conditions) (First evaluation of Directive 2001/29/EC, Bechtold, in Dreier/Hugenholtz, 2006).

In short, and to apply this provision in our case to this exception, in the absence of voluntary measures taken by the rightholders and if the enjoyment of the exception for the benefit of disabled people is prevented by the use of TPMs put on works, member states have to intervene with appropriate measures.

The relevant Greek provision (Article 66(A)(5) Law 2121/1993) states the following:

Notwithstanding the legal protection provided for in par. 2 of this article, as it concerns the limitations (exceptions) provided for in Section IV of law 2121/1993, as exists, related to reproduction for private use on paper or any similar medium (article 18), reproduction for teaching purposes (article 21), reproduction by libraries and archives (article 22), reproduction for judicial or administrative purposes (article 24), as well as the use for the benefit of people with disability (article 28A), the rightholders should have the obligation to give to the beneficiaries the measures to ensure the benefit of the exception to the extent necessary and where that beneficiaries have legal access to the protected work or subject-matter concerned. If the rightholders do not take voluntary measures including agreements between rightholders and third parties benefiting from the exception, the rightholders and third parties benefiting from the exception may request the assistance of one or more mediators selected from the list of mediators drawn up by the Copyright Organization. The mediators make recommendations to the parties. If no party objects within one month from the forwarding of the recommendation, all parties are considered to have accepted the recommendation. Otherwise, the dispute is settled by the Court of Appeal of Athens trying at first and last instance…."

Nevertheless the whole effect of this provision is soft pedaled by the last sentence of this provision (similar formulation as the fourth subparagraph of Article 6(4) Directive 2001/29) that provides differently in the digital networked environment: "These provisions shall not apply to works or other subject-matter 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." This provision limits the possibility to intervene in the "online" environment and take appropriate measures described in Article 66(A)(5). In those cases a total preeminence of the TPMs is given over the exceptions (Martin-Pratt, 2001, p. 75).

In the digital context, what is important is to extend these limitations and exceptions specifically to works regardless of their protection by TPMs. In other words,

neither the WCT (Article 11) nor the WPPT (Article 18) requires that TPMs be protected in a manner inconsistent with copyright's fundamental goals. Thus, the protection of TPMs can and should be circumscribed by appropriately tailored limitations and exceptions that include access for the benefit of print disabled in a digital context (Okediji, 2006).

## Conclusion

The issue is whether the existing legal national and the perspective international framework strikes the right balance between the legitimate interests of the creators and investors and print disabled people in the creation. This is something that the Greek legal framework tried to achieve; how successful or not the attempt is only the future and the copyright history will prove it.

No matter what solutions the national laws offer though, the ultimate solution should come at international level in order the cross border exchange of accessible formats to be dealt constructively. The barriers that print disabled people have to face are enormous but an optimistic air is blowing in the fields of copyright: new opportunities, legislative changes and the ongoing discussions in the international forum make us hope that this copyright problem will not remain long in the agenda.

## Endnotes

1. Article 19:

   "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

   "Article 27:

   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. 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."

2. These Rules were adopted by the General Assembly in 1993, available at http://www.un.org/esa/socdev/enable/dissre00.htm. Although not a legally binding instrument, the Standard Rules represent a strong moral and political commitment on the part of Governments to take action to attain equalization of opportunities for persons with disabilities. The rules serve as an instrument for policy-making and as a basis for technical and economic cooperation.

   The Standard Rules consists of 22 rules incorporating the human rights perspective which had developed during the decade preceding their adoption. The 22 rules concerning disabled persons consist of four chapters - preconditions and target areas for equal participation, imple-

mentation measures, and the monitoring mechanism - and cover all aspects of life of disabled persons.

Specifically Rule 5 provides in part as follows:

"Rule 5: Accessibility

States should recognize the overall importance of accessibility in the process of the equalization of opportunities in all spheres of society. For persons with disabilities of any kind, States should (a) introduce programmes of action to make the physical environment accessible; and (b) undertake measures to provide access to information and communication."

"Access to information and communication

Persons with disabilities and, where appropriate, their families and advocates should have access to full information on diagnosis, rights and available services and programmes, at all stages. Such information should be presented in forms accessible to persons with disabilities.

States should develop strategies to make information services and documentation accessible for different groups of persons with disabilities. Braille, tape services, large print and other appropriate technologies should be used to provide access to written information and documentation for persons with visual impairments.

States should encourage the media, especially television, radio and newspapers, to make their services accessible. States should ensure that new computerized information and service systems offered to the general public are either made initially accessible or are adapted to be made accessible to persons with disabilities.

Organizations of persons with disabilities should be consulted when measures to make information services accessible are being developed."

3. The Convention was adopted on 13 December 2006 and entered into force on 3May 2008 (http://www.un.org/disabilities/default.asp?id=150). Article 9 deals with a broad range of accessibility issues, Article 21 with the freedom of expression and access to information (among others the freedom to receive and impart information on an equal basis with others and through Braille and other accessible means), Article 30 focuses on participation in culture life (especially in par. 3 it is stated that States Parties are urged to take all appropriate steps, in accordance with international law, to ensure that laws protecting the intellectual property rights do not constitute an unreasonable or discriminatory barrier to access by persons with disabilities to cultural materials. it is aimed to ensure that when framing national copyright laws the needs of VIPs should be taken into account providing a balance. Finally, Article 32 refers to the international co-operation. Analytically:

"Article 9 - Accessibility

1. To enable persons with disabilities to live independently and participate fully in all aspects of life, States Parties shall take appropriate measures to ensure to persons with disabilities access, on an equal basis with others ... to information and communications, including information and communications technologies and systems ... These measures, which shall include the identification and elimination of obstacles and barriers to accessibility, shall apply to, inter alia:..

b) Information, communications and other services, including electronic services and emergency services.

2. States Parties shall also take appropriate measures:

a) To develop, promulgate and monitor the implementation of minimum standards and guidelines for the accessibility of facilities and services open or provided to the public;

b) To ensure that private entities that offer facilities and services which are open or provided to the public take into account all aspects of accessibility for persons with disabilities;

c) To provide training for stakeholders on accessibility issues facing persons with disabilities;...

f) To promote other appropriate forms of assistance and support to persons with disabilities to ensure their access to information;

g) To promote access for persons with disabilities to new information and communications technologies and systems, including the Internet;

h) To promote the design, development, production and distribution of accessible information and communications technologies and systems at an early stage, so that these technologies and systems become accessible at minimum cost."

"Article 21 - Freedom of expression and opinion, and access to information

States Parties shall take all appropriate measures to ensure that persons with disabilities can exercise the right to freedom of expression and opinion, including the freedom to seek, receive and impart information and ideas on an equal basis with others and through all forms of communication of their choice, as defined in article 2 of the present Convention, including by:

a) Providing information intended for the general public to persons with disabilities in accessible formats and technologies appropriate to different kinds of disabilities in a timely manner and without additional cost; ...

c) Urging private entities that provide services to the general public, including through the Internet, to provide information and services in accessible and usable formats for persons with disabilities;

d) Encouraging the mass media, including providers of information through the Internet, to make their services accessible to persons with disabilities. ..."

"Article 30 - Participation in cultural life, recreation, leisure and sport

1. States Parties recognize the right of persons with disabilities to take part on an equal basis with others in cultural life, and shall take all appropriate measures to ensure that persons with disabilities:

   a) Enjoy access to cultural materials in accessible formats;

   b) Enjoy access to television programmes, films, theatre and other cultural activities, in accessible formats; ...

2. States Parties shall take appropriate measures to enable persons with disabilities to have the opportunity to develop and utilize their creative, artistic and intellectual potential, not only for their own benefit, but also for the enrichment of society.

3. States Parties shall take all appropriate steps, in accordance with international law, to ensure that laws protecting intellectual property rights do not constitute an unreasonable or discriminatory barrier to access by persons with disabilities to cultural materials.

"Article 32 - International cooperation

1. States Parties recognize the importance of international cooperation and its promotion, in support of national efforts for the realization of the purpose and objectives of the present

Convention, and will undertake appropriate and effective measures in this regard, between and among States and, as appropriate, in partnership with relevant international and regional organizations and civil society, in particular organizations of persons with disabilities. Such measures could include, inter alia:

a) Ensuring that international cooperation, including international development programmes, is inclusive of and accessible to persons with disabilities;

b) Facilitating and supporting capacity-building, including through the exchange and sharing of information, experiences, training programmes and best practices;

c) Facilitating cooperation in research and access to scientific and technical knowledge;

d) Providing, as appropriate, technical and economic assistance, including by facilitating access to and sharing of accessible and assistive technologies, and through the transfer of technologies.

2. The provisions of this article are without prejudice to the obligations of each State Party to fulfill its obligations under the present Convention."

The Convention entered into force in May 2008 and till now 84 countries have ratified it. Greece is not among them. (See all relevant information at: http://www.un.org/disabilities/default.asp?navid=12&pid=150).

4. No other rights are mentioned because only those ones are governed by the Information Society Directive. This does not necessarily mean that there cannot be an exception also to other rights, such as the public performance right.

5. The European Accessible Information Network (EUAIN) is a EU funded project in which FEP participated alongside with EBU, academics and accessible formats producers. The project was established in 2004, when a core group of organizations involved in accessible content production came together on a European level to seek greater clarity and systematization for this field. The EUAIN Network has brought together the different stakeholders, including publishers and associations representing people with disabilities, in accessible content processing and sought to find new ways to mainstream the provision of accessible content, to design for convergence, to describe the practical advantages of moving from ideas of accessible to adaptive environments.

Based on this extensive work over, it has been possible to identify key trends in accessible content processing that are likely to be of some importance in the coming years, such as accessibility on demand; accessibility to be embedded within mainstream content creation and production processes at the earliest stages; that is, accessibility from scratch.In synthesis, EUAIN provides support, tools and expertise to enable the provision of accessible information. One tool developed by the EUAIN Network is the Demonstrator: this has been set up in order to illustrate the potential of accessible publishing, whose concepts underpin the EUAIN project. The Demonstrator can be used for producing different output formats on-demand, from the same well-structured input file.

As a roll out of the EUAIN Network, another project has been developed (which is still ongoing) under the name of ProAccess. This is a "network of networks" project funded under the Digital Literacy strand from within the eLearning strand of the Commission. Improving accessibility of educational material for visually impaired people is the main pillar of the ProAccess project.

This project aims at providing publishers and intermediaries in the e-learning value chain (libraries, schools, charities and associations devoted to impaired people) with practical guidelines and instruments for the production and use of accessible content in a more effective way both from the productive process and copyright standpoint.

Within the framework of the EU project ProAccess a set of guidelines have also been developed to help the drafting of contracts between rightholders, intermediaries and final users. These guidelines aim to provide operational instructions to publishers, producers or other content providers of works in accessible format for the purpose of acquiring works in accessible format and making them available to disadvantaged people, also through libraries and other institutions, in compliance with legal and contractual rules on intellectual property rights (Bergman-Tahon, 2009).

## References

Akester P. (2010), The new challenges of striking the right balance between copyright protection and access to knowledge, information and culture, online at http://unesdoc.unesco.org/images/0018/001876/187683E.pdf /accessed 14/09/2010

Bergman-Tahon A. (2009), Improving access to works for visually impaired persons, European Parliaments' Committee on Legal Affairs, online at http://www.informaticaverde.org/blog/wp-content/uploads/2009/11/access-works-visually-impaired-persons.pdf /accessed 14/09/2010

Bottis M., Access to Information for persons with disabilities, Ionian Law Review 2006, pp. 34-48 (In Greek).

Dakin H., and Wijesena, W. (2005), Access to Copyright Material by People with a Print Disability, Copyright Reporter, Vol 22 No 4, 104

Dreier T., and Hugenholtz, B. (2006), Concise European Copyright Law, Kluwer Law International

Friend C. (2009), Improving access to works for visually impaired persons, European Parliaments' Committee on Legal Affairs, online at http://www.europarl.europa.eu/document/activities/cont/200911/20091113ATT64499/20091113ATT64499EN.pdf /accessed 14/09/2010

Friend C. (2009a), Meeting the Needs of the Visually Impaired Persons: What Challenges for IP? online at http://www.wipo.int/meetings/en/2009/vip_ge/presentations/chris_friend.html /accessed 14/09/2010

Garnett N. (2006), Automated Rights Management Systems and Copyright Limitations and Exceptions, prepared for WIPO SCCR 14th Session, SCCR/14/5, online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_14/sccr_14_5.pdf /accessed 14/09/2010

Geiger C. (2007), The role of the three-step test in the adaptation of copyright law to the information society. e-copyright Bulletin UNESCO, online at: http://unesdoc.unesco.org/images/0015/001578/157848e.pdf /accessed 14/09/2010

Geiger C. (2007a), From Berne to National Law, via the Copyright Directive: The Dangerous Mutations of the Three-Step Test, European Intellectual Property Review, 29

Guibault L., et al. (2007) Study on the implementation and Effect in Member States' Laws of Directive 2001/29/EC on the Harmonization of certain aspects of copyright and related rights in the information society online at http://www.ivir.nl/publications/guibault/Infosoc_report_2007.pdf /accessed 14/09/2010

Hugenholtz B., and Okediji, R. (2008), Conceiving an international instrument on Limitations & Exceptions to Copyright, online at http://www.ivir.nl/publications/hugenholtz/limitations_exceptions_copyright.pdf /accessed 14/09/2010

Kaitlin M. (2010), WIPO Proposals Would Open Cross-Border Access to Materials for Print Disabled online at http://www.ip-watch.org/weblog/2010/05/28/wipo-proposals-would-open-cross-border-access-for-print-disabled/ /accessed 14/09/2010

Lung G. (2004), Copyright exceptions for the visually impaired: international perspective, online at http://archive.ifla.org/IV/ifla70/papers/177e-Lung.htm /accessed 14/09/2010

Martin-Pratt M. (2001), The Relationship Between Protection and Exceptions in the EU "Information Society" Directive, Adjuncts and Alternatives to Copyright, in ALAI, Congress, June 13-17, 2001, USA

Noel, W. (1985), Copyright problems raised by the access by handicapped persons to protected works online at http://unesdoc.unesco.org/images/0006/000651/065169eb.pdf /accessed 14/09/2010

Okediji R. (2006), The International Copyright System: Limitations, Exceptions and Public Interest Considerations for Developing Countries, online at http://www.unctad.org/en/docs/iteipc200610_en.pdf /accessed 14/09/2010

Ricketson S. (2003), Study on limitations and exceptions of copyright and related rights in the digital environment. SCCR/9/7, online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_9/sccr_9_7.pdf /accessed 14/09/2010

Ricketson S. (1987), The Berne Convention for the Protection of Literary and Artistic Works: 1886-1986, Kluwer Law International

Senftleben M. (2004), Copyright, Limitations and the Three-Step Test, Kluwer.

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 / accessed 14/09/2010

Torremans P. (2009), Choice of law in EU copyright directives in Research Handbook on the future of EU Copyright, Edward Elgar

Toshiyuki K., and Paulius, J. (2010), Intellectual Property and Private International Law, 18th International Congress on Comparative Law, Washington

Westkamp G. (2007), The Implementation of Directive 2001/29/EC in the member states, Part II online at http://www.ivir.nl/publications/guibault/InfoSoc_Study_2007.pdf /accessed 14/09/2010

Report of the Working Group on Access by the Visually and Auditory Handicapped to Material Reproducing Works Protected by Copyright January 1983/ UNESCO/WIPO/WGH/I/3

Visual impairment and blindness, Fact Sheet N°282 (2009), online at http://www.who.int/mediacentre/factsheets/fs282/en/ /accessed 14.09.2010.

WHO's International Classification of Functioning, Disability and Health (ICF) online at http://www.who.int/classifications/icf/en/ /accessed 14/09/2010

Green Paper, Copyright in the Knowledge Economy, Commission of the EC, COM(2008) 466/3, p. 16) available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0466:FIN:EN:PDF /accessed 14/09/2010

Report of the Panel, US Section 110(5) Copyright Act, 15 June 2000, WTO Doc. WT/DS/160/R, § 6.108 online at http://www.wto.org/english/tratop_e/dispu_e/1234da.pdf /accessed 14/09/2010

First evaluation of Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society (2007)

Workshop on Copyright: Tackling Orphan Works and Improving access to works for visually impaired persons (2009), online at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/juri/dv/juri_20091110_workshopprogramme_/juri_20091110_workshopprogramme_en.pdf /accessed 14/09/2010

Conclusions of the 17th SCCR (2008), online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_17/sccr_17_www_112533.pdf /accessed 14/09/2010

Conclusions of the 18th SCCR (2009) online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_18/sccr_18_conclusions.pdf /accessed 14/09/2010

Conclusions of the 19th SCCR (2009), online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_19/sccr_19_conclusions.pdf /accessed 14/09/2010

Supplementary information on the WIPO studies on limitations and exceptions SCCR/18/2 (2009), online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_18/sccr_18_2.pdf /accessed 14/09/2010

Analytical Document on limitations and exceptions SCCR/19/3 (2009) online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_19/sccr_19_3.doc / accessed 14/09/2010

Background Paper by Brazil, Ecuador and Paraguay on a WIPO Treaty for Improved Access for Blind, Visually Impaired and other Reading Disabled Persons (2009) SCCR/19/13/Corr., online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_19/sccr_19_13.pdf /accessed 14/09/2010

Proposal for a WIPO Treaty for Improved Access for Blind, Visually Impaired and other Reading Disabled Persons (2009) SCCR/18/5, online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_18/sccr_18_5.doc /accessed 14/09/2010

Background Paper by Brazil, Ecuador and Paraguay on a WIPO Treaty for Improved Access for Blind, Visually Impaired and other Reading Disabled Persons (2009) SCCR/19/13, online at http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=130505 /accessed 14/09/2010

Stakeholders' Platform: Interim Report (2009) SCCR/18/4, online at http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=122314 /accessed 14/09/2010

Stakeholders' Platform: Second Interim Report (2009) SCCR/19/10, online at http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=130394 /accessed 14/09/2010

Stakeholders' Platform: Third Interim Report (2010) SCCR/20/6, online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_20/sccr_20_6.doc /accessed 14/09/2010

EU Proposal: Draft Joint Recommendation concerning the improved access to works protected by copyright for persons with a print disability (2010) SCCR/20/12, online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_20/sccr_20_12.pdf /accessed 14/09/2010

Draft proposal of the USA for a consensus instrument to WIPO (2010) SCCR/20/10, online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_20/sccr_20_10.pdf /accessed 14/09/2010

Timetable for the Adoption of a WIPO Treaty for an Improved Access for Blind, Visually-Impaired and Other Reading Disabled Persons (2010) SCCR/20/9, online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_20/sccr_20_9.pdf /accessed 14/09/2010

Draft WIPO Treaty on Exceptions and Limitations for the Disabled, Educational and Research Institutions, Libraries and Archive Centers (2010) SCCR/20/11, online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_20/sccr_20_11.doc /accessed 14/09/2010

Report on the Questionnaire on Limitations and Exceptions (2010) SCCR/20/7 online at http://www.wipo.int/edocs/mdocs/copyright/en/sccr_20/sccr_20_7.pdf /accessed 14/09/2010

# Digital library's liabilities. Which law applies? Copyright infringement, blasphemy and hate speech

**Dimitris Sarafianos**

## Introduction

The act of digitizing and placing a copyrighted work in an e-library can qualify as a tort and raise numerous questions of applicable law[1]. Such acts can be tortious, for instance, if committed without the authorization of the author or the copyright owner. In such case, copyright is infringed both by uploading the copyrighted work to the worldwide web (unlawful reproduction) as well as by making the work available to the public through the internet. The mere placing of the work on the internet, however, can qualify as a tort in itself irrespective of copyright breach. This happens when in a given jurisdiction the publication of a work is against the law (e.g. when a work is considered to be blasphemous or to insult religion or to incite hatred on racist, national or religious grounds – hate speech). In such instances, liability lies not only with the creator of the work but with the distributor as well. In other words, the maker of an e-library is exposed to risks he may be unaware of as he cannot be sure to know all the laws which apply in all the countries from which access to the e-library (and through it to the work) is possible. Similar problems may arise in copyright since, as will be discussed below, there are cases where the maker of an e-library may believe to have acquired the required authorization but it may not be effective in all the countries from which access to the e-library (and through it to the work) is possible. So significant problems may arise not only due to the cost of copyright clearance or to orphan works but also from variances in the applicable law. In the first part of this article, we will proceed to examine the problems of private international law in copyright; in the second part, we will consider some issues of private international law arising from legislation on blasphemy and hate speech[2].

## Copyright and applicable law

The choice of applicable law in case of copyright infringement with a foreign element is a quite complicated matter on which there is divergence of opinion (in both doctrine and case-law) and is still in the process of international consideration on the road to a common arrangement [3]. On a series of substantive issues, such as the initial owner of copyright (especially in collective works), the

scope of the moral right, the limitations of copyright, etc. countries have adopted contradictory and conflicting rules. Even at community level where the process of harmonization of legislation has built up a rich *acquis communautaire* in copyright, significant differences continue to exist between jurisdictions. Therefore, the importance of applicable law in case of intra-community conflict of laws remains topical.

The legislator has three main options regarding the choice of law in tort liability[4]: the law of the country of origin of the work (*lex origini*), the law of the protecting country (*lex loci protectionis*) and the law of the country in which protection is claimed (*lex fori*)[5]. The legislator may also choose between adopting the same applicable law on all subject matters of copyright (ownership, existence, scope, legal remedies) or a different applicable law for each matter. The theoretical discussion on the issue is very rich, especially in countries without relevant express legislation. In general, however, we find that the options are usually limited between the *lex loci protectionis* and the *lex origini* (for unpublished works the latter is the law of country of the author's nationality; for published works, it is the law of the country of origin as specified in the Berne Convention[6]). The applicability of the *lex fori* is mostly limited to matters of legal procedure or public policy[7].

In Germany, for example, the prevailing view in both doctrine and case-law upholds (in combination with art. 120 UrHG) that all the legal aspects of copyright are governed by the law of the protecting country[8]. By contrast, in France it is accepted that the scope of copyright and, generally, the extent of protection are governed by the law of the protecting country whereas the copyright existence and initial ownership are governed by the law of the country of origin of the work[9]. In the US the initial ownership of copyright is governed by the law of the country of origin of the work while the scope and, in general, the extent of protection are governed by the law of the country for which protection is claimed[10]. In Greece, according to art. 67 Law 2121/1993, initial ownership, existence and scope of copyright are governed by the law of the country of origin of the work, while legal remedies are governed by the law of the country for which protection is claimed, but this rule applies only if the International Conventions on Copyright do not stipulate otherwise (Koumantos, 2002, pp. 67 sqq; Marinos, 2004, pp. 424 sqq.; Sarafianos, 2009, ar. 67/nr.3,50-59).

These differences persist despite the fact that all four countries have joined the International Convention of Berne which contains certain rules of private international law that will be discussed in 1.1. In community law, the issue of conflict of laws is dealt with in two ways: first, the EC Treaty itself and its article 12 which establishes the general principle of non-discrimination on grounds of nationality (see below 1.2). Second, the process of harmonization of private international

law rules by way of Regulations (as, in this case, Regulation 864/2007 on the applicable law to non-contractual obligations – Rome II) (see below in 1.3). The scope of this Regulation, however, is limited to harmful events that occur after its entry into force, i.e. after 11.01.2009. Besides, the adoption of Regulation Rome II falls short of solving all the thorny issues of private international law in the field of copyright, especially with regard to the internet.

### *Choice of law under the Berne Convention*

Considering that the US has joined the Berne Convention since 1989, China since 1992, Russia since 1995 and 163 other countries have joined it too, it becomes clear that, in most cases of copyright protection the applicable law is, in principle, that stipulated by the Berne Convention.

The Berne Convention does not contain a general rule of applicable law but a series of *leges speciales* depending on the issue at hand, i.e. copyright existence, ownership, scope, limitations, duration, etc (Fawcett & Torremans, 1998, p. 461; Ricketson & Ginsburg, 2006, p. 1299)[11].

The Convention aims at protecting foreign authors (i.e. authors whose works originate in countries other than the one in which protection is claimed). To that purpose, it establishes two basic tenets: the principle of national treatment on the one hand, and rules of minimum protection applicable to all foreign works, on the other hand (Ricketson & Ginsburg, 2006, p. 1297). Pursuant to art. 5 (1) of the Convention which contains these two principles, authors enjoy (in regard to works protected under the Convention in countries other than the country of origin of the work) a) the rights that the law of these other countries recognize or will recognize in the future (national treatment principle), as well as, b) the rights stipulated in the Convention (minimum rules).

The Berne Convention does not obligate countries to transpose the rights stipulated by it (minimum rules) in national legislation (as is the case with the community harmonization process). This means that national authors (that is, authors whose works originate in the protecting country) cannot claim these rights in their country –e.g. the country of origin of their works (see also art. 5 (3) (a) of the Convention, "Protection in the country of origin is governed by domestic law"). Thus, the application of the Convention may lead to increased protection for foreign authors (who may additionally claim the minimum rules stipulated by the Convention) compared to national authors (Fawcett & Torremans, 1998, p. 468) [12].

The principle of national treatment defines how foreign works are treated as explained above and should not be confused with the rules of applicable law contained in the Convention (v.Eechud, 2003, p. 107; Koumantos, 1988, p. 440; Lucas & Lucas, 2006, pp. 935 sqq.). The principle of national treatment can affect

the choice of applicable law in two ways: a) by contributing to the interpretation of the relevant provisions of the Convention, b) by preventing the application of a substantive rule which should apply according to a national choice of law rule but would lead to lesser protection of foreign *versus* national authors. Provided, of course, that such lesser protection do not result from the application of an express rule of private international law under the Convention (Ricketson & Ginsburg, 2006, p.319)[13].

In tort law which is our topic here the critical questions of private international law consist in the legal rules that will determine a) the existence of copyright, i.e. whether a work is protected by copyright law and the applicable qualifications of originality[14], b) the ownership of copyright, i.e. who is considered as the creator of the work, who as the copyright owner/holder and, mainly, who is legally entitled to claim damages for the infringement, c) the scope, limitations and duration of copyright which will determine if the act in question qualifies as tort or not (for instance, if a right is not deemed as absolute and exclusive but merely as a claim to a reasonable or statutory remuneration, failure to pay such remuneration does not automatically qualify as tort), d) the remedies for copyright protection including measures of interim protection, measures for the prevention or cessation of infringement and remedies to ensure indemnification.

## Existence of copyright

The Convention contains no rule of applicable law in regard to the existence of copyright. The national legislator remains free to stipulate which law will specify the qualifications of originality of the work or even whether the work will qualify for protection under copyright law. In all events, however, the application of the substantive rules of the law of the country of first publication (lex origini) may not lead to situations that violate the principle of national treatment. Thus, if the law of the country of first publication requires a higher degree of originality for a given category of works (e.g. photographs) than the protecting country, this particular rule of the law of the country of first publication will not apply for it leads to lesser protection of foreign *versus* national works. If, on the contrary, the law of the country of first publication requires a lesser degree of originality for a given group of works than the protecting country, then it will apply.

The only exception to the issue of existence is article 2 (7) of the Convention on designs and models. Under this provision if an industrial design or model or a work of applied arts qualifies as such in the country of origin and the protecting country has adopted a special legislative regime for these categories of works, then only the protection specifically reserved to designs and models can be claimed in the protecting country. If the protecting country has no special legislation on designs and models, then the application of copyright law can be claimed

for these works too although in the country of origin they do not qualify as works covered by copyright. According to this rule, the test for the applicability of special legislation on designs and models is not how the works are designated in the protecting country but how they are designated in the country of origin. Of course, nothing prevents the national legislator from adopting a system of cumulative protection so that these works are protected both based on the legislation on designs and models as well as based on copyright law insofar as they meet the qualifications required by the latter.

## Ownership of copyright

The Berne Convention contains no special rule of applicable law on the initial owner of copyright. The legislator remains free to specify the applicable law which will determine which person/s (individual or legal entity) is the first author or the first co-authors of the work.

There is one exception: the copyright owner in cinematographic and, generally, in audiovisual works. Under article 14 bis (2) (a) of the Convention, the copyright owner of audiovisual works is determined by the legislation of the country where protection is claimed (Ricketson & Ginsburg, 2006, pp. 388 sqq.). This provision attempts to reconcile the law of most jurisdictions in continental Europe that designate one or more physical persons as the author (director) or the co-authors (director, soundtrack composer, screenwriter) of the work with Anglo-Saxon jurisdictions that designate a legal entity (the production company) as the author or, at least, the co-author of the work. Instead of establishing a minimum rule to harmonize jurisdictions, it was left to each country to treat audiovisual works according to its own system of law provided all works (foreign and national) be treated equally (Fawcett & Torremans, 1998, p. 511)[15]. Thus, for example, the director of an audiovisual work which was first made accessible to the public in the US from a production company based in US may claim his rights as the author in Greece although in the country of origin of the work he is not considered as the author of the work. This compromise was met with strong criticism especially because, with this system, the author of the work changes every time the work crosses borders (Ricketson & Ginsburg, 2006, p. 1320).

At any rate, the holder of copyright – even if not recognized as the first owner – may claim his secondary contractual rights (in which case the corresponding rules of private international law will apply)[16] or invoke the presumptions on his protection as the copyright holder (on this see article 15 of the Berne Convention). Thus, for instance, although a US company – the producer of an audiovisual work – is not entitled under Greek law, for example, to claim the economic rights emanating from copyright in its capacity as first author of the work, it may rely either on the respective agreement for the assignment of copyright by the

director or claim that the work bears the required indication of copyright (a possibility which cannot apply, of course, for the inalienable moral right).

## Scope of copyright and remedies

The extent of protection and the legal remedies provided to authors to protect their copyright are governed exclusively by the legislation of the protecting country (art. (5) (2) (b)). The view currently prevailing on the international level (Desbois, Francon & Kerever, 1976, pp. 135-139; Fawcett & Torremans, 1998, p. 467; Katzenberger, 1999, pp. 1694, 1696; Koumantos, 1988, pp. 450-451; Lucas & Lucas, 2006, p. 954; Ricketson & Ginsburg, 2006, p. 1299; Ulmer, 1978, p. 11; contra Stewart, 1983, pp. 38-39) is that the protecting country is the country for which protection is claimed (*lex loci protectionis* – see also recital 26 Regulation 864/07) and not the country in which protection is claimed (*lex fori)*.

In addition to legal remedies (sanctions, enforcement) the extent of protection includes the scope of copyright (the recognition and content of economic and moral rights). The same is true about the limitations of copyright (Ricketson & Ginsburg, 2006, p. 316). It would be against the principle of national treatment (in applying the law of the country of origin) to deny protection to a work which is subject to increased limitations in the country of origin as compared to the limitations which are effective in the protecting country. But also in case where the country of origin applies fewer limitations, the application of the law of this country would lead to unfavorable results for the user of the work who might otherwise claim the application of the limitation. Besides, copyright limitations are either delimitations serving the same purpose that led to the granting of copyright (the development of cultural production – see especially the classical limitations in articles 10, 10 bis of the Convention) or a kind of statutory licenses against payment of a fair fee to the author which, being involuntary, are effective only within the jurisdiction that grants them (cf. articles 13 (1) and 11 bis (2) of the Convention).

The only exception to the scope of copyright under article 14 ter of the Convention is the *droit de suite*. In the context of the principle of reciprocity, protection can be claimed in all the countries that have adopted the *droit de suite* but only if the national legislation of the author has also adopted this right and only to the extent that it has (Koumantos, 1988, p. 445).

## Duration of protection

On the issue of duration of copyright, the Convention contains a special provision under which protection in the protecting country is governed by the law of the latter but cannot be longer than the duration of protection in the country of origin of the work unless the law of the protecting country specifies otherwise (art.

7 (8)). This principle (comparison of the terms of protection) always leads to the shortest term of protection. Thus, if the term of protection in the protecting country is shorter than the term of protection in the country of origin the term of the protecting country prevails. If the term of protection in the protecting country is longer than the term of protection in the country of origin the term of the country of origin prevails. This provision seems to take into account that if the work has already come into the public domain in the country of origin, protection cannot be claimed in another country (cf. art (18) on the application of the Convention on works created prior to its entry into force).

## Efforts to extricate an erga omnes rule of applicable law and their inconsistencies

With these methodological observations in mind we may now follow the international discussion which tries to extricate a single rule of applicable law from the Convention. One group of theorists (Katzenberger, 1999, Vor§120; Nimmer & Nimmer, 2001, §17.05; Plaisant, 1962, pp. 63-66; Troller, 1952, p.8; Ulmer, 1977, pp. 479 sqq.; Ulmer, 1978, p. 11, to name a few) argues that the Convention establishes as the applicable law on all issues (except the contractual exploitation of the work) the law of the protecting country (*lex loci protectionis*). Another opinion (Koumantos, 1988, pp. 448 sqq.; Koumantos, 2002, pp. 81 sqq.) argues exactly the opposite: that the Convention establishes as the applicable law on all issues (except legal remedies) the law of the country of origin (*lex origini*).

In most cases, the general applicability of the *lex protectionis* is based on the principle of territoriality. Although this principle is not explicitly enshrined in the Berne Convention, it is not entirely without merit in our opinion. Even though copyright is not granted by act of public authority (as is the case with trade-marks or patents) the protection of copyright is recognized through the national legislation of each country and acquires international content by countries joining international conventions (Fromm & Nordemann, 1998, Vor §120; Katzenberger, 1999, pp. 1693-1698). In actual fact, the principle of territoriality is a legal form of national sovereignty which applies to all legal rules. This, however, does not mean that we can, based on this principle, infer a general rule of applicable law[17]. The countries that choose to adhere to the Convention's regime accept the rules of applicable law it contains and apply their own rules of applicable law on all matters not regulated by the Convention (they may, therefore, refer to the law of another country - v.Eechoud, 2003, p 98; Schack, 1979, p. 25)[18].

What is more, we could not, based on a limited rule of applicable law (art. 5 (2) (b)), establish the grounds for the principle of territoriality itself so that we may then interpret this rule as generally applying in contrast to the systemics of the Convention (vicious circle).

In particular: no-one objects to the fact that in fields such as contractual obligations the Convention leaves the regulation of private international law matters to the national legislator of the protecting country (Ginsburg, 1998, p.26; Ulmer, 1978). Furthermore, if according to the Berne convention all matters of copyright were to be regulated by the law of the protecting country (in an expansive interpretation of the rule in art. 5 (2) (b)) it would have made no sense to include a provision to the effect that the copyright holder of audiovisual works is determined by the legislation of the protecting country (art. 14 bis (2) (a))[19].

What is more, it would have been unnecessary to make clear that non-compliance with copyright registration formalities - in those countries of origin where such a system is in place – does not prevent the enjoyment and exercise of copyright in the protecting country (art. 5 (2) (a)). It would have sufficed to mention that the country in which the protection of the work is claimed cannot impose as a requirement for the protection of foreign works the prior compliance with formalities. On the contrary, the fact that it is expressly stated that in this case (compliance with formalities) the rules of the law of the country of origin of the work do not apply seems to imply that Berne Convention countries consider the application of these rules possible in other cases[20].

Neither could a rule of choice of law be drawn directly from the principle of national treatment (for such a position see Dinwoodie, 2001, p.31; Nimmer & Nimmer, 2001, §17.05; Troller, 1952, p. 8). As mentioned earlier, national treatment regulates the treatment of foreign works without even assimilating the treatment of foreign to that of domestic authors since foreign authors can be treated more favourably as compared with domestic authors (who may not invoke the minimum rules of the Convention).

For the same reasons (i.e. because national treatment does not mean equal treatment), the principle of national treatment cannot be construed so as to lead to the adoption of the law of the country of origin (*lex origini*) as the applicable law in all cases[21].

It is also submitted that art. 5 (3) (a) of the Convention (pursuant to which protection in the country of origin is regulated by national legislation), establishes an imperfect rule of private international law which, if extended into a fully-fledged rule by interpretation, will apply on all matters of applicable law in copyright the law of the country of origin (Koumantos, 2002, p. 81)[22]. At first sight, this interpretation is not incompatible with the systemic interpretation of the Convention's express choice of law provisions (which would, in this case, be deemed as exceptions and, as such, would be interpreted narrowly), but it is doubtful whether such a rule can be inferred from an article (art. 5 (3) (a) of the Convention) created for an entirely different purpose: to prevent authors from claiming the rights

granted by the Convention (minimum rules) in their own country (Azzi, 2005, pp. 252-253; Fawcett & Torremans, 1998, pp. 474-475; Lucas & Lucas, 2006, p. 948)[23].

It is argued, finally, that when the Berne Convention makes reference to the applicability of the law of a specific country it refers not only to the substantive rules but also to the private international law rules stipulated in that law (Koumantos, 2002, p. 76; for a criticism, Koumantos, 1988, p. 451). This view is incompatible with the systemics of the Convention and can lead to a *regressus ad infinitum*. In fact, there can be no further referencing between the Convention and the law of the country referred to by the Convention. The country whose law is expressly referred to by the Convention may not in its turn refer to the law of another country because this would defeat the special purpose for which each rule of applicable law was included in the Convention; and the implications of further referencing might lead to the opposite result from that wanted by the Convention (in other words the violation of the principle of national treatment; Ricketson & Ginsburg, 2006, p. 1298; cf. Fawcett & Torremans, 1998, pp. 469, 473). Neither is further referencing conceivable for matters on which the Convention does not specify the applicable law and for whose regulation it does not refer to the law of a specific country (in this case the national legislator stipulates the applicable law for the first time). Further referencing is only thinkable between the law of two countries (i.e. the applicable law chosen by the national legislator and the law referred to by the applicable law chosen by the national legislator). But this risk has been explicitly removed in community jurisdiction with art. 24 Regulation 864/2007 Rome II on non-contractual obligations and art. 20 of Regulation Rome I on contractual obligations, and also art. 15 of the Treaty of Rome (1980) on contractual obligations.

### *Art 12 of the EC Treaty*

As is known, this article bans all discrimination on grounds of nationality. As has become accepted, this provision applies on matters of copyright too and obligates each member-state to ensure absolutely equal treatment between its subjects and the nationals of other member-states whenever community law applies (ECJ ruling 20-10-93, Phil Collins C-92/92, C-362/92, ECJ Index 1993, 5145).

It was upheld in this context (ECJ Ruling 6-6-02, Ricordi- La Boheme, case C-360/00, Index 2002, 5089) that the principle of comparison of the terms of protection adopted by German law (in implementation of art. 7 (8) of the Berne Convention) is against art. 12 (formerly 6) of the EC Treaty as it leads to discriminatory treatment between national and other community authors.

The ECJ extended the implications of this case-law with its ruling 30-6-2005 in Tod's SpA and Tod's France SARL *v.* Heyraud SA (case C-28/04, Index 2005, 5781). In this case, the Italian company Tod's who is the right holder of shoe models under the Italian law on designs and models requested the French court of the forum where their right was infringed to apply the provisions of French copyright law. French law (the law of the protecting country) indeed provides for a system of cumulative protection of designs and models, on the one hand, and copyright, on the other hand, especially for the creations of the clothing and jewelry industry (ar.112-2 (14) Code de la Propriete Intellectuelle). By contrast, Italian law (the law of the country of origin) excludes cumulative protection. Under art. 2 (7) of the Berne Convention, the Italian house is not entitled to claim this cumulative protection for shoes as they do not qualify as original works protected by copyright in Italy.

The ECJ expressly held in this case that the rule of art. 2 (7) of the Berne Convention is incompatible with art. 12 of the EC Treaty. Also, it expressly held that art. 12 of the EC Treaty does not allow a member-state to depend the admissibility of an author's lawsuit for the protection of copyright granted to him by the legislation of that state on considerations based on the country of origin of the work. As a result of this case-law, any provision adopting the law of the country of origin as the applicable law is not applicable on EU member-state nationals, at least not insofar as it concerns the existence of the work and the qualification of originality[24].

### *Regulation Rome II*

Since the implementation of Regulation 864/11-6-2007 on the applicable law on non-contractual obligations (Rome II) the relevant provisions of private international law of all member-states are unified (with the exception of Denmark). Under the rule of art. 8 of said Regulation, the applicable law on non-contractual obligations emanating from copyright infringement is the law of the country for which protection is claimed (*lex loci protectionis*). Furthermore, in case of copyright infringement, there will be no derogation from the principle of the *lex loci protectionis,* not even under art. 14 of the Regulation which allows the parties of the dispute to choose the applicable law (art.8 (3)).

This rule has universal application pursuant to art. 3 of the Regulation and, as a result, the law of the country for which protection is claimed will apply even if this country is not member of the EU.

Of course, the scope of this Regulation is limited to harmful events occurring after its entry into force. As a result, the provisions of the Berne Convention and the rules of private international law of each country which apply in case of conflict

of copyright laws remain effective with regard to harmful events which occurred prior to January 11, 2009.

Regulation 864/2007 will settle many ambiguities left by the interpretation of Berne Convention. First of all, art. 15 of the Regulation specifies that the applicable law on non-contractual obligations governs in particular, a) the basis and extent of liability, including the persons who may be held liable for their actions, b) the grounds for the exemption from liability as well as any limitations and division of liability, c) the existence, nature and assessment of damage or of the remedy claimed, d) the measures that can be taken to prevent or terminate the injury or damage or to ensure payment of damages within the limits of the ruling court according to the respective procedural law, e) the transferability of the right to claim damages or a remedy including succession, f) the persons entitled to compensation for damage sustained personally, g) liability for the actions of third parties, h) the various ways of extinction of obligations and the rules of prescription and limitation including the rules relating to the commencement, interruption or suspension of a period of prescription or limitation.

Considering that the issues regarding the scope of protection are regulated by the *lex loci protectionis* as discussed above, the question arises if this Regulation has any effect on matters that under Greek law (and the law of other countries) used to be governed by the law of the country of origin. The Regulation does not make explicit reference to matters of copyright existence and initial ownership. In our view, however, the fact that art. 15 of the Regulation expressly stipulates that the *lex loci protectionis* even governs who is entitled to claim compensation for damage sustained personally deserves particular attention. Moreover, given that the list in art. 15 of the Regulation is by way of indication and the wording of art. 8 seems to imply that the *lex loci protectionis* governs all issues arising from the non-contractual obligations emanating from copyright infringement, one may conclude that art. 8 (1) of the Regulation establishes what the Berne Convention avoided: a general rule for all copyright issues arising from copyright infringement[25].

In our opinion, this is also the best solution *de lege ferenda*. The major argument against a general application of the law of the country for which protection is claimed is that it seems to imply that the creation of copyright depends on its infringement[26]. Obviously, this is not right. In point of fact, copyright is created as soon as the work is created. And the law of some jurisdiction will apply from that moment: if the work remains unpublished, it is the law of the author/s' nationality; if it is published, it is the law of the country where the author/s has chosen to publish it. At any rate, however, the problem is not what law applies on the work from its creation to the moment of copyright infringement but what law applies in case the situation of the work acquires foreign elements. And this will happen

either when the use of the work becomes the object of contract or when copyright is infringed.

Anyway, the choice seemingly adopted by Regulation Rome II is still problematic in the modern era of the internet and of simultaneous cross-border transmission of copyrighted works for the tort in this case is perpetrated simultaneously in many countries.

If the problem of the forum that will settle the dispute in this case has been adequately addressed in the EU[27], the problem of applicable law on non-contractual obligations arising from the use of the internet or other cross-border acts remains a thorny one.

The whole discussion around the applicable law in case of simultaneous cross-border torts illustrates the problems of various solutions (Ginsburg, 1998, pp. 40 sqq; Koumantos, 1996, p. 251; Lucas, 2001, pp. 17 sqq., Ricketson & Ginsburg, 2006, pp. 1301 sqq.). If we choose the law of the country where the triggering event takes place (e.g. in satellite transmission the place of the up-link; on the internet the place of installation of the server) we run the risk of seeing piracy heavens sprouting around. According to one view, the less risky solution is the law of the country of professional installation of the infringer although again one should consider the leeway of off-shore companies[28]. Another view makes a distinction between cases where the copyrighted work is placed on the market through a particular website ("push technology") where the applicable law should be the place of installation of the website's server and the cases of peer to peer reproducers and video on demand ("pull technology") where the applicable law should be the law of the place from where the distribution of the work is requested (Ricketson & Ginsburg, 2006, 1310). By contrast, if we choose the place where the damage occurs, the application of this rule would lead to the concurrent application of the law of each protecting country (mosaic principle).

In our view, the safest option *de lege ferenda* would be to explicitly specify which law applies in each case of cross-border tort (as is the case, for instance, with EU Directive 93/83 on satellite transmission). Until that happens, however, the judge must apply the law of each country where the tort is committed, his only option being to apply the provisions of art. 4 of Regulation Rome II *mutatis mutandis* and try to limit the choice of law by considering a) if from the overall circumstances it may be concluded that the tort has an obviously close connection with one country (e.g. due to a pre-existing contract between the copyright owner and the infringer), b) if the owner and the infringer usually reside at the same country at the time the damage occurs, or, c) if the damage occurred only in a particular country/countries. Thus, the judge is called upon to choose the appropriate law taking into consideration all the circumstances of the case at hand.

In conclusion, if a work is included in an electronic data bank without the authorization of the author after 11-1-2009 and proceedings are brought within an EU member-state, the applicable law is the law of the protecting country (or countries). If this happened prior to the above date, the scope of copyright and the legal remedies will be governed by the law of the protecting country (or countries) but the existence and the owner of copyright will be governed by the law of the country indicated by the *lex fori*. Thus, in the above examples respectively, in Germany it will be the law of the protecting country, in France, US and Greece the law of the country of origin. The principle of comparison of the terms of protection will determine the duration of copyright. But if the work was created by a community national and the forum lies inside the EU, the duration and scope will be governed by the law of the protecting country. Finally, foreign law provisions will not apply if incompatible with a provision of public policy of the law of the forum, i.e. if a provision of foreign law is incompatible with the fundamental civil, moral, social, legal or economic perceptions prevailing in the country.

## Blasphemy, hate speech and applicable law

The problems encountered when one attempts to determine the applicable law in copyright are no more hard to solve than those arising when trying to determine the applicable law in case of violation of the provisions on blasphemy, religious insult and hate speech.

There is significant divergence among jurisdictions as to whether blasphemy, religious insult and hate speech qualify as offences or not (and under which circumstances), even as to whether those whose religious feelings or religious freedom are offended have cause to sue for damages.

By way of indication, for European countries we can mention the following[29]:

a) Blasphemy is an offence *inter alia* in Austria, Denmark, Finland, Greece, Ireland, Italy and the Netherlands. These countries also stipulate the offence of religious insult which qualifies as an offence also in Germany, Spain, Russia, Norway, Poland, Portugal, Iceland, Lithuania, Ukraine, Switzerland (whereas repealed in the UK, Sweden).

The qualifications vary from country to country. In Greece, Austria and Denmark it is not required that an actual person be offended for an act to qualify as blasphemy or religious insult. In Ukraine punishable is the insult against citizens' religious feelings. In Germany and Portugal the act must be capable of disturbing the public order for the offence to materialize. In Spain the act must provoke a great public scandal.

b) Conserning incitement to hatred or hate speech (e.g. a form of expression which spreads, incites, promotes or justifies hatred based on intolerance[30]) the international conventions that castigates the crime allows a certain degree of flexibility for every party's legislation[31]. Therefore, although incitement to hatred qualifies as an offence in practically all European countries, in some countries (such as Greece, Austria, Italy) the law punishes incitement to acts that are likely to create discrimination or violence and not mere hatred. In other countries negationism (e.g. the public denial of historical facts or genocide with a racial aim) is also a crime (France, Austria, Belgium, Switzerland[32]). In Turkey every public denigration of Turkishness is punishable. In the majority of member-states, the incitement to hatred must occur in public. In France, the fact that the incitement is committed in public is an aggravating circumstance. In Austria and Germany, the incitement to hatred must disturb the public order to qualify as an offence. Intention to stir up hatred is generally not a necessary element of the offence whereas it is so in Cyprus, Ireland, Malta, Portugal, Ukraine and England and Wales[33]. By contrast, in the US any legislation to that effect would be deemed as violating freedom of expression[34]

All the above provisions interfere with freedom of expression as enshrined in Art. 10 of the European Convention of Human Rights which protects even shocking or disturbing expressions of ideas[35]. Although the European Court of Human Rights has held that religious insult may in certain circumstances be regarded as malicious violation of the spirit of tolerance, which must be a feature of a democratic society[36], in fact this offence, as long as it penalizes forms of expression, constitutes a breach in the liberal context of the ECHR. Moreover, it actually promotes intolerance. The law seems to pay heed to the request of a religious community: do not provoke us or we will attack you or, even worse, resort to generalized violence[37]. All crimes of "arousing" citizens not falling within the scope of instigating crimes against specific material goods (life, physical integrity, property), namely not aiming at convincing others to commit acts they would not commit otherwise, but inciting to acts of violence indirectly and by reflex (in the sense that a violent act is the reflex response to such incitement) contain an oxymoron: their punishment leads to the satisfaction of the perpetrators of violent acts. Thus, the protected legal interest behind public (religious) order (which can be disrupted by acts of violence – and only by such) seems to be the intolerance of others, and in its more vicious form. This is undoubtedly the case with blasphemy and religious insult[38]. But the same could be said about some forms of hate speech that do not provoke nor aim to provoke violence against a person or group of persons on grounds of their race, colour, religion, language, national or ethnic origin. The depreciation or denigration of a

group of persons, even with a discriminatory intention, does not always provoke nor aim to provoke a violation of the rights of such persons[39].

As to civil law remedies it must be stressed that personality cannot possibly be infringed upon when the abuse or derision is not directed against a specific person and such person is deemed to be offended indirectly and by reflex (as member of a group - group libel)[40]. And even in the event of a direct offence of personality it must be investigated whether freedom of expression and freedom of art prevail through satire or criticism[41]. But since in many countries jurisprudence still castigates religious insult and religious hate speech (with the ECHR's blessings) we must answer to the question of which law applies.

On the international level, it is accepted that tort obligations are governed in principle by the law of the country where the tort was committed (*lex loci delicti commissi*). There are many occasions, however, (typically, the Internet) where the facts that make up the *actus reus* of an offence are committed in more than one country or the facts occur in one country but the consequences arise in another.

With regard to the offences we are concerned with, for instance, the question is whether one is entitled to claim damages for the injury suffered because of these acts. As we mentioned earlier, in our view, the answer is in the negative (especially for the offences of blasphemy and religious insult). But if such entitlement were accepted, the injury could be argued only as an offence against personality. The distinction has significant legal implications as Regulation Rome II does not apply on non-contractual obligations emanating from violations of privacy and personality-related rights including defamation (art. 1 (1) (h))[42]. In particular, should such acts be considered as offences against personality, the applicable law would decide if there are time limits for instigating proceedings and if the time limit starts anew with every new publication.

In any event, the applicable law on torts committed prior to the date specified by the Regulation depends on the legislation of each country[43].

Austria (art. 48 Bundesgesetz uber das Internationale Privatrecht 15-6-78) and Portugal (45(1) of the Civil Code) adopt the law of the country where the act that qualifies as tort was committed as the applicable law (*lex loci actus*). If the facts of the *actus reus* of the tort occurred in more than one country, the country where the tort was committed is the country in which the relevant acts were completed (e.g. the country of installation of the server where the work was uploaded). However in defamation cases Austria opts for the law of the place where the victim enjoys a reputation, presumed to be his habitual residence and Portugal for the law of the place where the damage is sustained when the lex loci actus does not provide for compensation. In France the applicable law is the law of the place

where the damage occurred (*lex loci damni*, e.g. the place where the work became accessible to the public). In defamation cases this means the place where the defamatory product was distributed and brought to the knowledge of third parties.

In Italy (art.62(1) Act 31-5-95), although the *lex loci damni* is the applicable law, the victim may request the application of the *lex loci actus*. In defamation cases this means that significant is the place where the defamatory product was published, but the victim has the right to opt for the law of the place of the publisher' s installation. If the parties reside in the same country, the law of the country of residence is the applicable law. By contrast, in Germany, although the applicable law is the *lex loci actus*, the victim may request the application of the *lex loci damni* (40 (1) EGBGB[44]). So the victim has the right to choose as connecting factor between the publisher' s headquarters or the place where the product was published. But should it be considered that another country has a closer connection with the facts of the case, then the law of that country applies (41 (2) EGBGB). If the parties reside at the same place, the law of the country of residence is the applicable law (40 (2) EGBGB). In case of more than one *locus damni*, the *lex loci* applies only for the actual damages that occurred in each country (mosaic principle)[45]. German law also contains a clause (38 EGBGB) to the effect that the law of the foreign country to be considered as the applicable law according to the above will not apply on German citizens if it entails greater liability as compared with the provisions of German law.

In the UK (sec. 11.2.c Private International Law (Miscellaneous Provisions) Act 1995) the applicable law is the law of the country the tort is most closely connected with, therefore, the judge is called upon to choose the appropriate law taking into account all the circumstances of the case at hand (the place where the damage occurred, the place of the act, domicile, residence and nationality of the parties, the place of professional activity). However, this principle does not applies in defamation cases[46]. In defamation cases, English courts have traditionally applied a "double actionability rule" which states that for an English court to give damages in respect of foreign publications the matter must be actionable both in England and in the country in which the publication takes place[47].

A similar regulation exists in the US (2nd Restatement 1971) and the judge is called upon to choose the appropriate law taking into account all the circumstances of the case at hand, but the relevant policies of the forum state and of other interested states as well as the basic policies that underlie a particular field of law are also considered as relevant factors for choice of law purposes.

In the Netherlands, art. 3 (2) of the Dutch Conflict of laws tort Act favours the *lex loci damni* but contains a foreseeability clause. And if another country is considered as having a more closely connection with the facts of the case, the law of

that country applies. If the parties reside at the same place the applicable law is the law of the country of residence (3 (3) Dutch WCOD).

If the Rome II Regulation is considered as applying in these cases then pursuant to art. 4 the general rule is that the applicable law is the law of the country where the damage occurred regardless of the country where the harmful event occurred, and also the law of the country or countries where the event causes indirect effects. However, if the alleged culprit and the injured party have, at the time when the damage occurred, their usual residence in the same country, the law of the latter applies. By way of exception, if all circumstances imply that the tort has an obviously closer connection with another country (as in the case of a pre-existing contractual relationship between victim and perpetrator) the law of the latter applies. Under art. 14 of the Regulation the parties may agree to apply a different law on non-contractual obligations after the occurrence of the harmful event[48]. In this case, however, if at the time the harmful event occurred, all the circumstances related to the event are located in a country other than the country whose law was chosen by the parties, the choice of the parties may not affect the applicability of mandatory law provisions of the former or, if it is a member of the EU, the applicability of community law which cannot be derogated from by private agreement (prohibition of circumvention).

From the above we can conclude that the exception of personality related offences from Rome II Regulation (although desired by both the organizations of publishers and journalists) creates great uncertainty as to the applicable law and the prerequisites of civil liability for the author of digital library. Group libel lawsuits can be more dangerous than simple defamation cases. It is therefore critical to reach a new settlement between the different positions so as to establish certainty and foreseeability of law.

## Endnotes

1. In this paper we examine e-library author as content provider and not as host or access provider (as in the case of link libraries). Of course, even this distinction poses questions of applicable law.
2. Problems of similar nature may arise in cases of violation of personal data, illicit competition, trade-mark abuse, etc. In all such cases, the right holder may claim damages for each infringement. Of course, what is relevant in terms of applicable law is tort, e.g. when in addition to criminal liability the perpetrator also bears civil liability. And this because in criminal liability the applicability of the lex fori is not put in question (v.Eechoud, 2003, p.29).
3. See WIPO Forum on Private International Law and Intellectual Property, 2001; Drexl & Kur (eds.), 2005, passim.
4. In this article we do not examine choice of law issues in copyright contracts nor infringements of related rights for which see Azzi (2005), pp. 248 sqq.; Fawcett & Torremans (1998), pp.

572 sqq.; Guibault & Hugenholtz (2002); Lucas (2001); Lucas & Lucas (2006), pp. 836 sqq., 901 sqq.; Metzger (2005) pp.61 et seq.; Rickertson & Ginsburg (2006), pp. 1323 sqq.

5. The distinction between the lex loci protectionis and the lex fori is significant because the infringement of copyright can occur in a country other than the country where the defendant has his domicile. Usually the plaintiff has the right to choose between the jurisdiction of the defendants' domicile and the jurisdiction of the place of tort (for EU countries see art. 5§3 of Regulation 44/2001).

6. The country of origin of the work is deemed to be (art. 5 (4) of the Convention): i) if the work was published for the first time in a Berne Convention country, that country; ii) if the work was published simultaneously in more than one Berne Convention countries each of which has a different rule on the duration of copyright protection, the country whose legislation grants the shortest term of protection; iii) if the work was published simultaneously in a country outside the Berne Convention and in a Berne Convention country, the Berne Convention country; iv) if the work was not published or was published for the first time in a country outside the Berne Convention without simultaneous publication in a Berne Convention country, the Berne Convention country of which the author is a national; v) in any event, if it is a cinematographic work whose producer has his professional installation or usual residence in a Berne Convention country, that Berne Convention country; if it is a project of architecture which was erected in a Berne Convention country or a work of the graphic or the fine arts incorporated in a structure situated in a Berne Convention country, that Berne Convention country. It should be noted that the notion of publication under the Convention is restrictive. Pursuant to art. 3 (3) of the Convention, publication is considered as first publication if done (cumulatively): i) with the author's consent, ii) in some sort of physical fixation of the work regardless of the manner of manufacture, iii) in a number of copies available to the public (in any way whatsoever, e.g. through sale, lease, donation) which satisfies the reasonable needs of the public depending on the nature of the work. The same article proceeds to exclude from the notion of publication the performance of a dramatic, dramatico-musical or cinematographic or musical work, the public recitation of a literary work, the communication by wire or the broadcasting of literary or artistic works, the exhibition of a work of art and the construction of an architectural work.

7. According to art. 26 of Regulation 864/2007 (Rome II) . A classical example of implementation of the public policy rule is the Huston case in France (Cour de Cassation 28-5-1991, JCP G 1991, II, 21731).

8. BGH 17-6-1992 "Alf" GRUR Int 1993, 258; BGH 2-10-97 "Spielbankaffaire" GRUR Int 1998, 427; BGH 29-4-1999 "Laras Tochter" I ZR 65/96; Katzenberger (1999), Vor§120 pp. 1691 sqq. esp. 1693 - 1698.

9. Cour de Cassation 22-12-1959 "Ridau de fer", D. 1960, 93; Cour de Cassation 28-5-1991. "Huston", supra note 7; Desbois (1964), pp. 34 – 36; Lucas & Lucas (2006), pp. 791 sqq.

10. Itar-Tass Russian News Agency v. Russian Kurier, Inc. 153 F.3d 82 (2d Cir. 1998).

11. For the dissenting opinions see below under 1.1.5.

12. In this sense, the principle of national treatment can not be deemed as a non-discrimination principle.

13. Correspondingly, art. 3 of the TRIPS Agreement and its relevant note according to which every member of the Agreement extends to the nationals of the other parties a treatment

that is no less favourable compared with its own nationals with regard to the protection of copyright (such protection meant as covering the availability, acquisition, scope, maintenance and enforcement of copyright) specify the scope of the principle of national treatment. Hence, the provision concerns the way foreign nationals are treated and not the applicable rules of private international law; see Fawcett & Torremans (1998), pp. 481, 509 sqq., especially 512, according to whom the provision does not exclude, even if exceptionally, the application of the lex origini or the lex fori on some of the issues, particularly the initial ownership of copyright (see also Torremans, 2005, p. 76).

14. For a long time it was questioned, for instance, whether data bases or software programs qualify for protection under copyright. See Bottis M., Information Law, Nomiki Vivliothiki, 2004 and Bottis M., The legal protection of databases, Nomiki Vivliothiki, 2004 (in Greek). Today, respectively, it is questioned whether a multimedia work should be protected primarily as an audiovisual work or a data base or a software program (Stamatoudi, 2002). As to the degree of originality required for a work to qualify for protection under copyright law, the example of photographs is typical. Many countries (as for example Greece) require a lesser degree of originality to protect photographs as works qualifying for copyright protection whereas in other countries (such as Germany) only photographic works enjoy full copyright protection (for the distinction between photografic works –Lichtbildwerke- and photographs –Lichtbilder see §2 (1) 5 and §72 UrhG.).
15. For a strong criticism on this compromise see Desbois,Francon &.Kerever (1976), pp. 216-221.
16. Berne Convention does not contain choice of law rules on contractual obligations. Applicable are the relevant private international law rules of every country and for EU countries the new Rome I Regulation (593/2008) for contracts signed after 17/12/2009 and the Rome Convention of 1980 on the law applicable to contractual obligations for contracts signed before this date.
17. Besides, the principle of territoriality could in its turn raise a host of relevant connective factors: place of nationality, place of usual residence, place of creation, place of publication (Koumantos, 1988, pp. 441 sqq; Koumantos, 2002, p. 66 fn. 153; Lucas, 2001, p 3; Shack, 1979, p. 20).
18. Besides, unlike criminal law where the judge applies the law of the forum, in case of art. 5 (2) (b) the judge of the forum is called upon to apply the law of the protecting country (lex protectionis) which does not necessarily coincide with the law of the forum – thus the argument that thanks to the lex loci protectionis (and in contrast to the lex origini) the judge has a better knowledge of the law he will apply holds no water (for this approach see Stewart, 1983, pp. 38-39).
19. Even if this argument cannot be founded on the discussions that preceded the regulation (Ulmer, 1977, p. 499 points out that there was no conversation on the applicable law when the provision was adopted) the systemics of the Convention speaks in favour of the a contrario argument.
20. Especially concerning the existence of copyright; for the relevant discussions on the adoption of the article see v.Eechoud (2003), pp. 69-70.
21. Koumantos (1988), pp. 451 claimed that the principle of national treatment should be considered as imposing the equal treatment of foreign and national works both in terms

of copyright and in terms of applicable law (thus, if in the protecting country the law of the country of origin applies on national works – since the two coincide in this case – then, accordingly, the law of the country of origin must apply on foreign works also); see also Koumantos (2002), p. 76.

22. On the inductive extraction of private international law rules from imperfect law provisions, see, in detail, Koumantos (1964), p. 98.

23. And because this is the meaning of that article and not the stipulation of a choice of law rule, the problem pointed out by Shack (1979), pp. 29 sqq. and v.Eechoud (2003), p. 109 does not arise. In the related example, where a Swiss citizen who publishes his work in Germany brings a law suit in Germany for copyright infringement in Switzerland, applicable is the Swiss law.

24. See a critic on this decision in Lucas & Lucas (2006), pp. 1052-1053.

25. For the relevant discussion see Drexl (2005), pp. 151 sqq., especially 176.

26. For the relevant discussion see Lucas & Lucas (2006), pp. 872 sqq.

27. The matter of jurisdiction is determined by art. 5 (3) of the Brussels-Lugano Conventions according to the interpretation of this provision by the ECJ in its ruling 7-3-1995 in case C 68/93 (Fiona Shevill, ECJ Index 1995, 415). According to this interpretation the injured party may bring proceedings either to the courts of the place where the culprit has his professional installation and claim damages for the overall injury incurred in all the countries where the tort was committed or to the courts of each country from where the tort was committed (e.g. each country from where access to the pirate copy of the work was possible) and claim damages only for the injury incurred in that country (the same direction is followed by art. 5 of Regulation 44/2001: Lucas, 2001, p. 14; Fawcett & Torremans, 1998, pp. 152 sqq., critically especially pp. 161,167-9; Ricketson & Ginsburg, 2006, p. 1295). It can be concluded from the above that in the second case the applicable law is the law of the protecting country (lex loci protectionis). The problem persists in the first case when the plaintiff files the suit in the place where the defendant has his professional installation and seeks damages for the overall injury incurred in all the countries. In this case one of the leges loci protectionis has to be chosen. On the contrary in Anglo-Saxon counties jurisdiction is determined by whether it can objectively be considered that the infringer indented to provide access to the website at issue to consumers of the country of the forum; see Court of Appeals 4th Cir. S.K.Young vs New Haven (available at http://pacer.ca4.uscourts.gov/opinion.pdf/012340.P.pdf); also -indirectly- High Court of Australia Dow Jones &Company Inc. v Gutnick (available at www.kentlaw.edu/perritt/courses/civpro/Dow%20Jones%20&%20Company%20Inc_%20v%20Gutnick%20%5B2002%5D%20HCA%2056%20(10%20December%202002).htm); DeGroote & Derroitte, 2003, pp. 66 sqq. In US for every single publication of a communication that produce damages only one action for damages can be maintained and all damages suffered in all jurisdictions can be recovered in this one action (§ 577 of 2md Restatement of Torts 1977 –single publication rule).

28. Although v.Eechoud (2003), pp. 218-219 considered it to be a small danger in view of the international conventions and the fact that the generation and circulation of information usually take place in the developed world where copyright enjoys increased protection.

29. An analytic report on various legislations can be found in Council of Europe/Venice Commission (ed.), 2008, pp. 61 sqq.

30. ECHR 4-12-2003 Gunduz v. Turkey.

31. The Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, provides that each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the distributing, or otherwise making available, racist and xenophobic material to the public through a computer system, but a Party may reserve the right not to attach criminal liability to such conduct, where the material advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. Notwithstanding this exception a Party may reserve the right not to attach criminal liability to such conduct to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies. Additionally this Protocol provides that each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the threatening or public insulting, through a computer system, of (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics, but a Party may either: a require that the offence has the effect that the person or group of persons is exposed to hatred, contempt or ridicule; or b reserve the right not to apply, in whole or in part this article. The same applies in the case of negationism. According to art.6 of the Protocol each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right the distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, or of any other international court established by relevant international instruments but a Party may either a. require that the denial or the gross minimisation is committed with the intent to incite 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, or otherwise b. reserve the right not to apply, in whole or in part, this article altogether.

32. Correspondingly the German Constitutional Court 90 BVerfGE 241 (1994) stated that the dissemination of false information (at least if its publisher knows that the information is false or its falsity has been proved) cannot claim the coverage of freedom of expression.

33. For the adventures of the English provision see Barendt (2005), pp. 178-179.

34. In *Brandenburg vs Ohio* (1969), the Supreme Court upheld the right of the Ku Klux Klan to call publicly for the expulsion of African Americans and Jews from the United States, even though the speech in question intimated the desirability of using violence. "The constitutional guarantees of free speech and free press," the Court wrote, "do not permit a State to forbid or prescribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless actions and is likely to incite or produce such action" (pp. 571–572). The Brandenburg test has proven nearly impossible to meet. For example, in the famous Skokie cases (*National Socialist Party of America v. Village of Skokie*,

432 U.S. 43 1977), Supreme Court affirmed the right of Nazis to march on a public street in a community populated with World War II concentration camp survivors. And in *R.A.V. vs City of St.Paul* (1992) invalidated an antibias ordinance under which several teenagers were convicted of burning a cross on an African American family's lawn. As Justice Antonin Scalia, reasoned "[t]he First Amendment does not permit St. Paul to impose special prohibitions on those speakers who express views on disfavored subjects. ... In its practical operation, moreover, the ordinance goes even beyond mere content discrimination, to actual viewpoint discrimination" (p. 391). Consequently online hate speech will rarely be punishable under the Brandenburg test. Moreover US Courts and legislative bodies protects US writers and editors even from the enforcement of foreign libel decisions. On the subject see Davidson (2008); Warshow (2006); *Telnikoff v. Matusevitch,* 702 A.2d 230 (Md. 1997); *Yahoo vs La Ligue Contre Le Racisme et L'Antisemitisme case* (433 F.3d 1199 (9th Cir. 2006) and especially New York's Libel Terrorism Protection Act, which gives American defendants protection from the enforcing of foreign libel judgments.

35. ECHR 7-12-1976 *Handyside vs UK;* 8-7-1986 *Lingens vs Austria,* 29-3-2001; *Thoma vs Luxembourg;* 31-1-2006 *Giniewski vs France.*

36. ECHR 20-9-1994 *Otto-Preminger-Institut vs Austria.* In broad strokes, the case-law of the ECHR on matters of protection of religious peace and religious feeling comes in contrast with its case-law on the protection of freedom of expression leaving a great margin of appreciation to national legislators. As typically stated (ECHR 25-11-1996 *Wingrove vs UK,* 10-7-2003 *Murphy vs Ireland,* 13-9-2005 *IA vs Turkey*) «The fact that there is no uniform European conception of the requirements of the protection of the rights of others in relation to attacks on their religious convictions means that the Contracting States have a wider margin of appreciation when regulating freedom of expression in connection with matters liable to offend intimate personal convictions within the sphere of morals or religion». See critically Alivizatos (2008), p. 256; Tsakyrakes (2006); Tulkens (2008), p. 311.

37. As the ECHR states in Preminger case (supra note 50), "the Court cannot disregard the fact that the Roman Catholic religion is the religion of the overwhelming majority of Tyroleans. In seizing the film, the Austrian authorities acted to ensure religious peace in that region and to prevent that some people should feel the object of attacks on their religious beliefs in an unwarranted and offensive manner".

38. For a more detailed analysis see Sarafianos (2008), p. 291.

39. See for example ECHR 13-1-2005 *Dogtekin vs Turkey;* 5-12-2002 *Kucuk vs Turkey* (but on the other hand 8-7-1999 *Surek vs Turkey*).

40. This is also the opinion of Greek Supreme Court (Areios Pagos 1298/2002 NoB 2002, p. 2064). On the contrary, in Preminger case ECHR has held that "The respect for the religious feelings of believers as guaranteed in Article 9 ECHR can legitimately be thought to have been violated by provocative portrayals of objects of religious veneration". With this jurisprudence religious feeling is reified. It is immanent in the public domain and can be infringed upon without the intervention of actual people. It is as if there were a legal fiction to the effect that the state itself has religious feelings. This is a blatantly ideological construct and cannot offer sufficient grounds for criminal punishment, as is the case for all non-personalized "feelings" (citizens' sense of security, etc.). It must be notes that in a more recent case (31-10-2006 *Klein vs Slovakia*) ECHR ruled that strong criticism against the head of a national church cannot be considered to be an insult against all members of this church. In US the Supreme

Court also ruled (in *Beauharnais vs Illinois*) that since an individual's dignity and reputation are associated with that of the group to which he belongs, there is no justification for treating group libel laws differently from the rules of private libel, but this jurisprudence remains unique since no case managed to pass the Brandenburg test (supra note 47). For this case see Barendt (2005), p. 184.

41. Especially in the area of artistic expression ECHR in many cases applied art. 10 of the Convention (24-5-1988 *Muller and other vs Switzerland;* 8-7-1999 *Karatas vs Turkey;* 29-3-2005 *Alinak vs Turkey)* and stated that "taken literally certain passages might be construed as inciting readers to hatred, revolt and the use of violence (…) it must nevertheless be borne in mind that the medium used was a form of artistic expression that appeals to a relatively narrow public compared to the mass media". As to the limits of this jurisprudence see ECHR 22-10-2007 Lindon, Otchakovsky-Laurens and *July vs France*.
42. The initial draft of the Regulation (art. 7) adopted as applicable law in cross-border personality-related torts the law of the country of residence of the offended party. This provision was fiercely objected to by publishers and journalists who whished to have as applicable law the law of the country of publication and/or of the country where the publications are mostly expected to circulate (on the related discussion see Warshow, 2006. On the reactions of publishers and journalists see www.epceurope.org/issues/RomeII_Joint_Position_for_Second_Reading.pdf, www.edri.org/edrigram/number3.13/RomeII). In the end, it was decided to leave these offences outside the scope of the Regulation.
43. See Commision's Proposal for Rome II Regulation COM(2003) 427 final 2003/0168 (COD)
44. BGH "Benomyl" NJW 1981, 1606.
45. OLG Hamburg NJW-RR 1995, 790.
46. see sec. 13 Private International Law (Miscellaneous Provisions) Act 1995.
47. *University of Glascow vs The Economist* 1997 EMLR 495, 501 sqq. See also Collins, 2005, pp. 370, 375-376.
48. The German EGBGB contains a similar provision (art. 42).

## References

Alivizatos, N. (2008). Art and religious beliefs: the limits of liberalism, in Council of Europe/Venice Commission (ed.), Tackling blasphemy, insult and hatred in a democratic society, pp. 255-258

Azzi, T. (2005). Recherche sur la loi applicable aux droits voisins du droit d'auteur en droit international prive, Paris: L.G.D.J.

Barendt, E. (2005). Freedom of Speech, 2nd edition, Oxford: Oxford University Press

Bottis M., Information Law, Nomiki Vivliothiki, 2004 (in Greek)

Bottis M., The legal protection of databases, Nomiki Vivliothiki, 2004 (in Greek)

Collins, M. (2005). The law of defamation and the internet, Oxford: Oxford University Press

Davidson, S. (2008). International Considerations in Libel Jurisdiction (available at www.forumonpublicpolicy.com/archivespring08/davidson.pdf)

DeGroote, B. & Derroitte, F. (2003). L'Internet et le droit international prive: un marriage boiteux?, Revue Ubiquite-Droit des technologies de l'information, pp. 61-82

Desbois, H. (1964). Les droits d'auteur et le droit international prive francais, Eranion in honorem G.Maridakis, vol. C, pp. 29-46

Desbois, H., Francon, A. & Kerever, A. (1976). Les conventions internationals du droit d'auteur et des droits voisins, Paris: Dalloz ed.,

Dinwoodie, G. (2001), Private international law aspects of the protection of trademarks, WIPO Forum on Private International Law and Intellectual Property (available at www.wipo.int/edocs/mdocs/mdocs/en/wipo_pil_01/wipo_pil_01_4. doc)

Drexl, J. (2005). The proposed Rome II Regulation: European Choice of Law in the field of intellectual property in Drexl, J. & Kur, A. (eds.) (2005). Intellectual Property and Private International Law (Heading for the future), IIC Studies vol. 24, Oxford and Portland, Oregon: Hart Publishing,

v.Eechoud, M. (2003). Choice of law in copyright and related rights: alternatives to the lex loci protectionis, The Hague-London-N.York: Kluwer Law International

Fawcett, J. & Torremans, P. (1998). Intellectual Property and Private International Law, Oxford: Clarendon Press

Fromm, F.K. & Nordemann, W. (1998). Urheberrecht. Kommentar zum Urhebergesetz und zum Urheberrechtswahrnemungsgesetz, Stuttgart: Kohlhammer (Ver.)

Ginsburg, J. (1998). Aspects de droit international prive de la protection d'oeuvres et d'objets de droits connexes transmis par reseaux numeriques, OMPI Groupe de consultants sur les aspects du droit international prive de la protection des oeuvres et des objets de droits connexes transmis par reseaux numeriques mondiaux (available at www.wipo.int/edocs/mdocs/mdocs/fr/wipo_pil_01/wipo_pil_01_9. doc)

Guibault, L. & Hugenholtz, P.B. (2002). Study on the Conditions Applicable to Contracts Relating to Intellectual Property in the European Union, study commissioned by the European Commission, Amsterdam: Institute for Information Law

Katzenberger, P. in Schricker,G. (1999). Urheberrecht Kommentar, Muenchen: C.H.Beck (Ver.)

Koumantos, G. (1964). Problems of international protection of copyright, Eranion in honorem G. Maridakis, v. C, pp. 91-118

Koumantos, G. (1988). Le droit international prive et la Convention de Berne, Le droit d'auteur, pp. 439-453

Koumantos, G. (1996). Les aspects des droit international prive en matiere d'infrastructure d'information, Koinodikion, pp. 241-253

Koumantos, G. (2002). Intellectual Property, Athens-Komotini 2002: A.Sakkoulas (ed.)

Lucas, A., (2001) Private International Law aspects of the protection of works and of the subject matter of related rights transmitted over digital netaworks, WIPO Forum on Private International Law and Intellectual Property (available at: www.wipo.int/edocs/mdocs/mdocs/en/wipo_pil_01/ wipo_pil01_1_prov.doc)

Lucas A. & Lucas, H-J. (2006). Traite de la Propriete litteraire et artistique, Paris: Litec (ed.)

Marinos, M. (2004). Intellectual Property, Athens-Komotini: A.Sakkoulas (ed.)

Metzger, A. (2005). Transfer of rights, license agreements and conflict of laws: remarks on the Rome Convention of 1980 and the current ALI draft in Basedow, J. & Drexl, J. & Kur, A. & Metzger, A. (eds). (2005). Intellectual Property in the Conflict of laws, Tuebingen: Mohr Siebeck (Ver), pp. 61-77

Nimmer, B.& Nimmer, D. (2001). Nimmer on Copyright, New York: Mathew Bender (ed.)

Plaisant, R. (1962). L'exploitation du droit d'auteur et les conflits des lois, RIDA, pp.63-109

Rickertson, S. & Ginsburg, J.C. (2006). International copyright and neighbouring rights (The Berne Convention and beyond), Oxford-New York: Oxford University Press

Ulmer, E. (1977). Gewerbliche Schutzrechte und Urheberrechte im internationalen Privatrecht, RabelsZ, pp. 479-514

Ulmer, E. (1978). Intellectual property rights and the conflict of laws, Deventer: Kluwer ed.

Sarafianos, D. (2008), Blasphemy in the Greek Orthodox legal tradition, in Council of Europe/Venice Commission (ed.), Tackling blasphemy, insult and hatred in a democratic society, pp. 287-292

Sarafianos, D. (2009) Art. 67 in Kotsiris, L. & Stamatoudi, E. (eds.), Law on Intellectual Property, Athens-Thessaloniki: Sakkoulas (ed.)

Shack, H. (1979). Zur Anknupfung des Urheberrechts im internationalen Privatrecht, Berlin: Duncker & Humblot (Ver.)

Stamatoudi, E. (2002), Multimedia products as copyright works, Cambridge: Cambridge University Press

Stewart, S.M. (1983). International copyright and neighbouring rights, London: Butterworths ed.

Torremans, P. (2005). Which law applies? A reply from Professor Torremans to Philip Johnson's reply to his earlier work, Journal of Intellectual Property Law & Practice, 2005, pp. 76-78

Troller, A. (1952). Das internationale Privat- und Zivilprozessrecht im gewerblichen Recthshutz und Urheberrecht, Basel: Verlag fur Recht Und Gesellshaft

Tsakyrakes, S. (2006), Religion vs Art, Athens: Polis (ed)

Tulkens, F. (2008). Les conflits entre droits fondamentaux: regards croises sur les art. 9 et 10 de la Convention Europeen des Droits de l' Homme, in Council of Europe/Venice Commission (ed.), Tackling blasphemy, insult and hatred in a democratic society, pp. 301-312

Warshow, A. (2006). Uncertainty from abroad: Rome II and the choice of law for defamation claims (available at www.brooklaw.edu/students/journals/bjil/bjil32i_warshaw.pdf)

# Digitization of works and access to culture: recent developments in Google Books and Europeana

**Maria Sinanidou**

## Introduction

The continuous and rapid development on the digitization projects both in the case of Google Books and Europeana show how access to culture - in whatever form, such as books, music, audiovisual works, photos - has now taken a new dimension through the web. Important issues in relation to copyright law but also regarding culture accessibility, civil rights, competition arise. Additionally, through the globalization process, regional cultures have become integrated through a global network of communication.

Taking as a start the Google Book digitization project one could bring to his mind Nikolai Gogol's story, the *Dead Souls*. Chichikov, its main character, travels around the Russian countryside to buy 'dead souls', so that he can become a wealthy and influential man. In the early 19th century Russian landowners had to pay annual taxes on the number of serfs (counted as 'souls') they owned as of the last census. Chichikov offered to buy 'dead souls' (i.e. serfs who had died since the last census) from the landowners. His plan was to acquire enough of these souls so that he could take out a large loan secured by his portfolio, and thereby to become a wealthy man.

In Gogol's story, Chichikov's scheme falls apart. Rumors are spread that the souls he owns are all dead and he flees the town in disgrace. Thus, this story makes one wonder about Google Books' and Europeana's future. Is it possible that Google's digitization project may pay off handsomely, as the Settlement – as we discuss it here later - would, in effect, give Google the exclusive right to commercially exploit millions of orphan books? How could this scheme affect Europeans and their projects?

## What is Digitization?

Digitization is the exchange of information, data, or works in a form capable of being processed by a computer, i.e. in binary code communication.

Digitization ensures high quality copies, provides ample opportunities for further processing, helps to copy an unlimited number and is characterized by a high rate of transmission of reproduced material.

In terms of copyright protection, digitization is a reproduction and as such requires the consent of the rightholder.

Why digitize?

There are two main reasons for digitizing material: to provide the widest possible access for the general public; and to ensure their survival.

It is crucial to examine what the types of works are that are interesting for the digitization project. There are three types of works:

### *Works protected by copyright*

These works are the ones publishers sell more active and they are available in most bookstores or through the Internet and libraries.

### *Works protected by copyright, but exhausted*

The books have been exhausted, cannot be issued or sold, so the only way to identify them is in a library or bookstore with used (second hand) books. Included are orphan works, i.e. out of print titles under copyright protection whose rightholder cannot be found.

### *Works that are not protected by copyright*

For example, the duration of protection has expired.

The issues resulting from digitization project depend on the nature of works. These will be illustrated on the example of Google's digitization project and the Europeana project.

## The controversial Google Books project

Google has scanned the texts of more than 10 million books from major university research libraries for its Book Search initiative and processed the digitized copies to index their contents. Google allows users to download the entirety of these books if they are in the public domain (about 1 million of them are), but at this point makes available only "snippets" of relevant texts when the books are still in copyright unless the copyright owner has agreed to allow more to be displayed (Bottis).

With over 70% of the US search market, Google's dominance amounts to monopoly power under the antitrust laws. Google's revenues exceeded $21 billion last year, and through its search results and sponsored links it controls indirectly hundreds of billions of dollars of other companies' revenues.

Here is how the project works: Once a book is scanned, it is added to Google's database and categorized depending on the book's copyright status. "If the text is no longer protected by copyright, the entire book is available for online viewing or download. However, if a book is still under copyright, only 'snippets,' or three-four line text sections, are available unless the rights holder has opted out completely or consented to a broader display, such as certain pages or chapters." Google's bold strategy was to scan now and negotiate later.

Soon after its inception, the Google Books project provoked a lawsuit claiming largescale copyright infringement. In late 2005, the Author's Guild of America, which at that time had 8000 members and the Association of American Publishers filed a class action lawsuit against Google in the Southern District of New York for copyright infringement. Google raised a fair use defence in answer, arguing that scanning and displaying portions, or snippets, of a book are permitted infringements of the owners' copyrights.

On October 28, 2008, the parties reached a Proposed Settlement Agreement. By the time the Proposed Settlement was submitted to the court, Google had scanned upwards of seven million books.

The U.S. Federal Court decided that a revised text of the Agreement should be presented. In a review meeting held on October 2009, the Court determined the 09.11.2009 as the date for the submission of an amended Settlement and on 13.11.2009 finally the modified version was presented.

## The Google Book Settlement

The Settlement consists of the creation of a system that allows for further creation of a database containing the full text of books scanned by Google, for commercial use in different ways. This new system involves giving rightholders the right to decide whether and to what extent it will allow Google to use their works against damages.

The Settlement covers books and inserts (even if a work is part of the Public Property or of Government Documents) which are protected by copyright and are digitized until 05/01/2009.

Excluded are photos, graphic designs, artworks, illustrations (no children) and other visual works included in the book, unless the rights holder of the optic project is the same as the rights holder of the text. Also excluded are journals, personal and government documents and projects that have ended the term of protection by copyright.

The book should either be:

a) issued in the U.S. and declared to the Directorate of Intellectual Property (US Copyright Office) until 05.01.2009 or

b) issued in Canada, or Australia, or the UK until 05.01.2009

## Distribution

63% (initially 70%) of the digital book sales will go to publishers.
Google will keep the remaining 37%.
Google will pay 63 percent of all revenues earned by such uses into a Settlement Class Fund ("Fund"), administered by the Registry, for the rights holders of the works. Google is required to pay a minimum of $45 million into the Fund for those rights holders whose works will have been digitized prior to the opt-out deadline.

On September 18, 2009 the Antitrust Division of the Department of Justice filed a first Statement of Interest ("Statement") formally objecting to the Proposed Settlement, particularly provisions that raised questions of price-fixing and other cartel-like behaviour under Sherman Act Section 1. In light of the concerns raised by the Antitrust Division, particularly those related to antitrust law, the parties began to consider amendments. Then on February 4, 2010, the Antitrust Division filed a second Statement with the court raising additional concerns, particularly about the proper bounds of class action settlements and the resulting market entry barriers. The Antitrust Division as well as interested third parties have filed numerous briefs with the court and published commentaries across the Internet. We will discuss briefly the class action question before proceeding to the antitrust issues.

Those authors and publishers who want to refrain from Google Books (opt out) can send a written request for their work to be removed from the Settlement.

According to the Google Book Settlement, if an author opts out, he will not be included in the Settlement, he will not receive the benefits conferred by the settlement and he will retain the right to sue Google and the Participating Libraries.

If he opts out of the settlement, he will neither be eligible for a Cash Payment or to participate in any of the revenue models under the Settlement, nor will the settlement's restrictions or obligations on Google or the Participating Libraries apply to his books and inserts.

Google has advised the Settlement Administrator that its current policy is to voluntarily honor such requests and refrain from digitizing books or, if they have already been digitized, refrain from displaying them.

Google is not able to digitize works of beneficiaries who have published in four countries (US, UK, Canada or Australia) and have expressly stated that they wish to participate in the Settlement. The above beneficiaries may remain in the Settlement either by not doing anything - which means it automatically covered by the terms of the settlement - or can choose exactly what applications can do with Google works.

### *What is the Book Rights Registry?*

The Registry will be a not-for-profit entity that represents the interests of rightholders in connection with this Amended Settlement with Google as well as potential licensing deals with other entities, subject to rightsholders' authorization. The Registry will have equal representation of the Author Sub-Class and Publisher Sub-Class on its Board of Directors, and will include at least one author and publisher representative from each of the US, Canada, the UK and Australia. The Registry will also delegate to an independent fiduciary responsibility for the exploitation of unclaimed Books and Inserts under the Settlement.

The Book Registry will give authors and publishers who give their consent for the digitization of their books a percentage of total revenue from the sale of electronic books and the accompanying advertisements.

In fact - and according to the parties to the Settlement - this register is somehow a new collecting society, which will administrate the rights of the beneficiaries.

### *How will the Registry be funded?*

To fund the establishment and initial operations of the Registry, and to pay for the costs of the Class Notice Program and claims administration costs, Google agreed to pay US $34.5 million, of which Google has already paid $12 million. On an ongoing basis, the Registry will be funded by taking an administrative fee as a percentage of revenues received from Google.

### *What will the Registry do?*

The Registry will:

- Represent the interests of the rightholders in connection with the Amended Settlement;
- Establish and maintain a database of contact information for authors and publishers;
- Use commercially reasonable efforts to locate rightholders;
- Distribute payments received from Google for the rightholders' share of revenues; and

- Assist in the resolution of disputes between rightholders.

In order to give effect to the Settlement this must be approved by the competent court of the United States (New York). The final hearing is scheduled for early 2010.

When the Amended Settlement is finally approved by the Court and no longer subject to any appeal it will be posted on website.

## Evaluation of effects on Copyright, Culture and Competition

### *Copyright*

The new text books published only in the EU (excluding UK) are excluded from the Settlement. Only books registered in the US Copyright Office (Copyright Division) or published in the UK, Australia or Canada fall within the scope of the Settlement, leaving only the titles of these features will be available through the service of Google.

The message is clear: Books published in countries of the delivery of copyright will be available through the service Google Book, while other jurisdictions in the tradition of droit d 'auteur (Europe and Asia) will remain outside.

Since there are also covered European works that are included in the US Copyright Office until 05.01.2009, this means that also some European rightholders fall under the Settlement. However, there is no data on how many European works have been published in the USA, Canada or Australia or how many are registered at US Copyright Office.

Before 1978 there were no electronic entries in US Copyright Office. So if one wants to determine whether a particular project was registered before 1978 in the US Copyright Office, he should travel to the USA in order to examine the natural records of the Copyright Office.

Until 1989, there are many works that have been filed in the US Copyright Office. This testimony is very helpful to the person who has the burden of proof in a copyright infringement. However, because of the Berne Convention (which provides copyright protection without any formalities) deposits in the US Copyright Office have been reduced.

A question of adequate representation of beneficiaries in the Register arises (only members of publishers from the UK, Australia, USA and Canada). Rest of beneficiaries will be individually negotiated to become parties to the Service.

Disadvantage: The beneficiaries that are not members of the class cannot be part of the Arrangement.

## Commercial Availability

Another important term is Commercial availability. In the past it was defined as follows: Only projects that are not commercially available can be fully displayed without the prior authorization.

Now the seller may be anywhere but the channel of trade should be available in the U.S., Canada, Australia, the UK.

A book is commercially available if, at the time in question, the book is offered for sale new by a seller anywhere in the world to a buyer in the United States, the UK, Canada or Australia.

If a book is designated as commercially available then Google will not be authorized to make any display uses of the book unless a rightholder of the book gives express permission to do so.

If a book is designated as not commercially available, then Google will be able to make all display uses of the book unless a rightholder of the book instructs Google to exclude the book from one or more display uses.

Thus there is a grey zone: What about books that were digitized before 13.11.2009 with the previous version of the Arrangement, and which (books) belong to publishers who are no longer in this class?

Google's answer: Not any compensation has been paid yet, so there is no question of compensation for damages.

## Orphan works and undistributed profits

Orphan works are out of print titles with copyright protection, whose rights holders can't be found. Google and its partners would not have to share the revenue for access to these books, which opponents say could number in the millions. Google says the number will be much less.

A broad consensus exists about the desirability of making orphan works more widely available. Yet, without a safe harbour against possible infringement lawsuits, digitization projects pose significant copyright risks.

Profits will be disposed after five years to identify the beneficiaries and will be redistributed among the already known rightholders or for other functions of the Registry.

After 10 years the Registry may ask the court for distribution to nonprofit organizations of beneficiaries.

Also, the Registry will appoint a custodian to represent the beneficiaries and protect their rights and give permission to others to the limit allowed by law.

A further issue which is raised is the question of compliance of the Settlement with international treaties (especially the Berne Treaty), under which the protection is independent of formalities. On the other hand, in the case of the Settlement, which is a private initiative, registration plays an important law.

Another issue that appears is the question of whether further agreements that might exist in other jurisdictions may limit the protection granted in US projects and US beneficiaries themselves with the conditions contained in the revised text of Settlement for non-US projects and non-US rightholders.

### *Culture*

Based on an evaluation of the Google Book digitization (Bearman, 2006, p. 2) there are some important issues that derive for digital libraries. These are the following:

1) Google will not be able to digitize everything ever printed, so its selection might favour American or English language sources over other cultures.

2) Google's presentation of texts based on keywords de-contextualizes them in culturally damaging ways and its primary interest in harvesting words to link to advertising permits sloppy imaging of the books at the expense of more carefully executed efforts.

3) The Google search engine promote search results that are not consistent with the rankings that scholars from the cultures in which the literature was written would approve.

4) Permitting a private firm to own the digital library of images and texts is not a sound archival plan for the world's libraries or cultures, and defeats efforts to encourage value-added exploitation of this unique resource.

5) Google's approach to copyright threatens the achievement of a universal digital library.

Over the past two years, Google has adopted downloadable PDFs for out of copyright protection volumes. But the fact that images of books digitized under the Google Book Search project are now visible increases the concern of librarians and scholars. The quality of the scans that have been made public is so poor that one could plausibly argue that they are part of Google's defence against copyright infringement, supporting the claim that the use made by automatic indexing is fundamentally different from making a copy (Bearman, 2006, p. 2).

Librarians seem caught in ambivalence these days about Google Book Search project (http://books.google.com), which is currently rolling up to (or past) 8 million books. The next major event in the project's history - the court's approval or disapproval of Google's settlement terms with authors and publishers over copyright issues - will decide whether millions more of those books will become available to all or part of the public. The American Library Association (ALA) and the Association of Research Libraries (ARL) have already sent a 'hot/cold,' 'yes/no,' 'go, but carefully' recommendation to the court. (http://wo.ala.org/gbs/wp-content/uploads/2009/05/googlebrieffinal.pdf). The document seems to blow hot and cold, complimenting and congratulating Google on its magnificent gift to the world, while at the same time raising fearsome doubts about Google as a commercial monopoly. The concerns expressed in the ALA/ARL document regarding the settlement are arranged in six sections: a) creates an essential facility with concentrated control, b) could limit access to the institutional subscription database (ISD), c) will heighten inequalities among libraries, d) does not protect user privacy, e) could limit intellectual freedom and f) could frustrate the development of innovative services.

The University of Michigan Libraries, on the other hand, has already made its approval clear by signing a contract that presumes the Settlement Agreement will go through as planned. In that agreement, however, the university has addressed some of the concerns expressed by librarians, which could set a standard for future agreements and allay concerns between librarians and mighty Google.

The Google Book Search program, particularly the library contributions that dominate the collection and include both in-copyright and out-of-copyright protection books, was challenged in the courts by both authors and publishers. Before courts could reach decisions on the matter, a settlement agreement was made by all parties. However, the settlement agreement needs the approval of the court, particularly since part of the settlement involves releasing millions of in-copyright/out-of-print and possibly orphan-works to the general public under subscription arrangements with institutions and a limited, free access route for public libraries. (For details on the settlement agreement, read the NewsBreak, "The Google Book Search Settlement: 'The Devil's in the Details,'" Nov. 3, 2008, http://newsbreaks.infotoday.com/NewsBreaks/The-Google-Book-Search-Settlement-The-Devils-in-the-Details-51429.asp.)

## *A copyright protection aspect*

The attitude that Google took to copyright was obviously not acceptable in Europe, and the disrespect to authors illustrated by Google's actual digitization since then is inconsistent with European notions of the moral rights of authors.

No public body in Europe could do other than engage in a discussion with authors and publishers to arrive at mutually acceptable terms under which to digitize its print heritage.

It has been criticised that Google made too little effort to find a solution that did not require courts to rule on the question of whether what they are doing violates copyright, because either decision will leave us worse off. If Google loses, all sorts of automated processes for adding value to texts could be foreclosed. If Google wins, we can expect future publishers to include more technical and legal methods of protection that permit the copyright owners to allow or disallow various forms of use, including reading, based on contract and protected by the Digital Millennium Copyright Act (DMCA) and similar legislation (Bearman, 2006, p. 4).

Google's project is indeed a brave project in digitizing the world's printed literature. The biggest challenge in this digitization is to keep the balance between copyright and the right of users for access to content.

Beyond Google there are also some other models being realized, in part in opposition to Google, such as the European Digital Library, European Search Engines and model library digitization endeavours.

### *A 'right to display the work publicly' aspect*

To perform or display a work publicly means to perform or display it anywhere that is open to the public or anywhere that a 'substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered.' Transmitting a performance or display to such a place also makes it public. It does not matter whether members of the public receive the performance at the same time or different times, at the same place or different places. Making a work available to be received or viewed by the public over an electronic network is a public performance or display of the work (e.g. *Kelly v. Arriba Soft Corp.*, 280 F.3d 934 (9th Cir. 2002); *Playboy Enters., Inc. v. Frena,* 839 F. Supp. 1552 (M.D. Fla. 1993).

The law distinguishes between ownership of the work as such (original or copy) and ownership of the copyright. A museum that acquires a painting does not thereby automatically acquire the right to reproduce it. Libraries and Archives commonly receiving books, scripts, or donations of manuscripts generally own only the physical copies and not the copyright.

Copyright is not absolute; it is subject to a number of limiting principles and exceptions. One of these exceptions is for example the exception for certain archival and other copying by libraries and archives. In the USA according to section 108 of the Copyright Act, libraries and archives are permitted to make up to three

copies of an unpublished copyrighted work 'solely for purposes of preservation and security or for deposit for research use in another library or archives'. The work must be currently in the collections of the library or archives and any copy made in digital format may not be made available to the public in that format outside the library premises. Libraries and archives may also make up to three copies of a published work to replace a work in their collections that is damaged, deteriorating, or lost, or whose format has become obsolete, if the library determines that an unused replacement cannot be obtained at a fair price. Copies in digital format, like those of unpublished works, may not be made available to the public outside the library premises.) In the European countries (for example in Greece, according to article 22 of Law 2121/1993 on copyright protection) 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.

Even if copying a work is not expressly allowed by law, it may still be permitted under the fair use doctrine (USA) or the three step test (Europe). However, the privileges under the fair use doctrine and the three step test do not replace any contractual obligation a library may have with respect to a work that it wishes to copy (Besek, 2003, p. 5). In any case the purpose and character of the use is very essential. Among the considerations is whether the use is for commercial or for non-profit educational purposes. Whereas in the States, under the fair use doctrine, the amount and substantiality of the portion used play an important role (generally, the more that is taken, the less likely it is to be fair use, but there are situations in which making complete copies is considered fair), in Europe this is irrelevant. Under the three step test applied in Europe the limitations on the economic right shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other protected subject-matter and do not unreasonably prejudice the legitimate interests of the right holder.

### *A 'right of access' aspect*

According to the 'Paperboy' decision of the BGH (BGH 17.7.2003, Az. I ZR 259/00, NJW 2003, p. 3406, see also Ott, 2004, p. 32; Ott, 2009, 556) there is no public access to a work taking place through a hyperlink. In another decision of the LG München I in 2007 the court decided differently for the case of a framing link( LG München I, decision 10.1.2007, Az. 21 O 20028/05, MMR 2007, 260) According to this decision it depends on whether the constructor of a webpage makes a work of another author appear as his own one. In that case the

person putting the framing link is making the work public accessible and a common user does not recognize that it is actually a work of a third person.

In 2008, in the case 'Rapidshare', the LG Düsseldorf decided that the right of making available to the public is infringed when the download link is published. Before the publication it is very difficult to find the work and the URL cannot be guessed (see also decision of the OLG Köln, Urteil vom 21.9.2007, Az. 6 U 86/07, MMR 2007, 786 ff.). From the 'Paperboy' and the 'Rapidshare' decisions, it is obvious that there are two acts necessary to make a work accessible to the public: upload and putting a link to the page where the uploaded work has been put (for more see: Ott, 2009, p. 359).

The new models indicate the need for increased availability of works protected by copyright in a growing number of consumers. Therefore it is an important step in the digitization and access to culture.

If approved, the Settlement will significantly increase the number of English language books available to U.S. users for online usage.

Financial incentives and obligations of the Registry will reduce the number of orphan works will bear on their surface, their parents.

However, most stakeholders agreed that the Settlement widens the gap between the U.S. and Europe regarding online (online) access to scientific and educational material and cultural heritage. This highlights the urgent need for similar projects (such as that of Google) in Europe.

It is immediate need to intensify efforts to digitize materials and museums, archives and libraries in Europe, to make accessible the material and the Europeans. It is therefore necessary to strengthen the European digital library Europeana and to allow access for Europeans in the protected material on orphan works.

Organizations of European librarians raise the issue in terms of public interest. Though recognizing the importance of the project, they argue that the deposition of global knowledge in the hands of a private company of US interests without the necessary control has some risks for the freedom of expression, research and cultural diversity.

Others, like James Grimmelman, professor at the New York Law School, argue that the Google Books Settlement contains risks for privacy as it allows Google to gather information about what one is reading.

### *Competition*

The Settlement is between Google, publishers and authors. Therefore, theoretically, Google's competitors can not benefit from the Settlement in their relationship with publishers and authors. They will have to make a similar Settlement to ensure similar conditions.

The U.S. Department of Justice conducted a survey on the potential impact of the agreement between Google, publishers and writers and recommended to the court in New York to reject the agreement will allow Google to digitize millions of books to commercial use in Internet.

According to the US Ministry of Justice, the agreement raises issues of copyright but also monopoly issues and should be rejected in its current form because it will give the power of Google on books, of which the holder can still be found and will fail provide adequate protection to foreign recipients.

It is notable that Microsoft, with Amazon and Yahoo! also react because they believe that ratification of the agreement would create a monopoly in the publishing sector worldwide.

Additionally it will give Google the power to limit price competition, which can lead other publishers of digital books off the market.

A competition issue that arrises concerning the Google Books project is whether a class action settlement in litigation between private parties is an appropriate vehicle for making public policy (for more see Peritz, R.J. and Miller M. (2010), An Introduction to Competition Concerns in the Google Books Settlement, New York Law School Legal Studies).

We should admit that if there is actually a need for amendments of the European legal framework, such amendments should be prepared in an open and transparent process with input from all concerned parties. International copyright rules cannot be changed in a settlement among US parties before a US Court.

Opponents say Google could gain a competitive advantage, potentially bolstering the power of Google search using the contents of millions of out of print books.

## The European response: Europeana (the European digital library)

Google's decision in 2004 to digitize books has been the main cause for reaction from Europe. Specifically, the National Library of France raised the issue first to create something like Google from Europe itself to have a balance.

Virtually the only way Europe would get a comparably broad license as the Settlement would give Google was to start its own project to scan books.

On 20.11.2008 the European digital library Europeana was launched. It is a gateway website that allows internet users to search and get direct access to digitised books, maps, paintings, newspapers, film fragments, and photographs from Europe's cultural institutions. About 7 million digitised objects are currently available and the number is expected to rise to 10 million in the course of 2010.

During 2009-2011, the EU's eContent plus programme will cover about 80% of Europeana's budget (€ 2.5 million per year). The Member States and cultural institutions will contribute the rest. Until 2013 the European Commission can continue supporting Europeana with €9 million through its Competitiveness and Innovation Programme. The office of Europeana is hosted by the National Library of The Netherlands in The Hague and is run by the European Digital Library Foundation.

On September, 30th 2005 the European Commission published the i2010: Communication on digital libraries, where it announced its strategy to promote and support the creation of a European digital library, as a strategic goal within the European Information Society i2010 Initiative, which aims to foster growth and jobs in the information society and media industries. The European Commission's goal for Europeana is to make European information resources easier to use in an online environment. It will build on Europe's rich heritage, combining multicultural and multilingual environments with technological advances and new business models.

Europeana.eu is about ideas and inspiration. It links people to 6 million digital items.

- Images - paintings, drawings, maps, photos and pictures of museum objects
- Texts - books, newspapers, letters, diaries and archival papers
- Sounds - music and spoken word from cylinders, tapes, discs and radio broadcasts
- Videos - films, newsreels and TV broadcasts

Some of these are world famous; others are hidden treasures from Europe's museums and galleries, archives, libraries and audio-visual collections.

The system used by traditional libraries for lending material is not suitable for the digital environment. In addition, the prior consent of the holder of property rights is needed before material can be made available online, except where the material is in the public domain. Consequently, a European library will basically have to concentrate on public domain material. In some cases, the costs of establishing the IPR-status of a work will be higher than the cost of digitizing it and bringing it online. This is particularly true for so-called 'orphan works' – films

or books for which it is impossible or very difficult to determine who holds the rights.

Improving online accessibility also requires appropriate multilingual services to allow users to explore and work with the content.

In its Recommendation 2006/585/EC on the digitization and online accessibility of cultural material and digital preservation (Official Journal L 236 of 31.8.20060, the Commission calls on Member States to speed up the digitization and online accessibility of cultural material (books, films, photographs, manuscripts, etc). To this end, Member States are encouraged to:

- collect information for producing overviews of digitization;
- develop quantitative targets for digitization;
- create public-private partnerships for funding purposes;
- develop facilities for large-scale digitization;
- endorse the European Digital Library;
- improve the conditions in which cultural material is digitized and accessed online.

Furthermore, the Commission is recommending that Member States take steps to further the digital preservation of cultural material by:

- setting-up national strategies and action plans, and exchanging information on these;
- establishing appropriate legislative provisions for the multiple copying and migration of digital material, as well as for the preservation of web-content;
- creating policies and procedures for the deposit of digital material, with due consideration given to the measures of other Member States.

The European Parliament Resolution on 'Europeana, the next steps', based on a report by German MEP Helga Trüpel, underlines the potential of the site as a common access point to Europe's collective heritage and calls on Member States to bring more digitized content into Europeana.

Today, Europeana (www.europeana.eu) gives direct access to 7 million digitized objects from Europe's cultural institutions, up from 2 million at its launch in November 2008. Some 37.4% of the digitized items come from France, followed by Spain with 13.2%, but content from some Member States is very limited, and masterpieces from many EU countries are still missing.

The Parliament's Resolution also addressed other issues that have to be tackled to ensure the success of Europeana, including the need to:

- address a series of copyright related issues to facilitate the digitization and online accessibility of cultural content. The report highlights in particular the issue of orphan works (works for which it is impossible to locate the copyright holders)
- ensure sustainable funding for the site
- raise awareness about Europeana among the general public and potential contributors.

Particular attention was paid to create the legal framework for rapid scanning solution for the so-called 'orphan' works. At the same time the desire has been expressed to extend the digitization and other forms of cultural expression and to support the Arrow system for identifying beneficiaries and certifying so-called orphan works.

It has been stressed that the aggressive policy of Google can be treated effectively by Europe only if we open up the Europeana project throughout the public sector from all over the world, always with a peak view of European culture.

During the meeting of Ministers in Charge of Culture and Audiovisual Policy in the framework of the Education, Youth and Culture Council November 27th, Ministers addressed the wider challenges for digitizing books and other cultural content, and making this material available through Europe's digital library Europeana (online at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/526&type=HTML&aged=0&language=FR&guiLanguage=en).

## Governance and funding of Europeana

On 28 August 2009, the European Commission adopted a Communication on "Europeana – next steps" outlining the key challenges that will determine its further development (IP/09/1257).

Following the Commission's Communication on Europeana, the EU ministers will exchange views on a series of key issues, such as the most appropriate financing model for Europeana, the possible involvement of private organizations (eg through sponsoring or advertising), and future governance structures for Europeana.

Orphan works represent a significant part of collections of cultural institutions in Europe (The British Library estimates that 40% of the collections protected under copyright law are orphan works). The Commission will examine this phenomenon through a detailed impact assessment.

The aim is to create a European-wide solution which will facilitate the digitization and distribution of orphan works and common standards of 'diligent search'

in order to identify the status of orphan works all over the EU. In this respect there has been some progress with the project ARROW (Accessible Registries of Rights Information and Orphan Works - Accessible records information on rights and orphan works), financed by the European Commission under the eContent plus (2,5 million), which brings together national libraries, collecting societies and publishers.

## Copyright Issues

Despite the significant progress made to date, there are still significant problems associated with the process of digitization and copyright law remain and seek an immediate solution.

Currently, Europeana includes mainly digitized books that are public domain, so no longer protected by copyright law (which lasts until 70 years after the death of the author).

The fragmented legal framework in Europe on copyright hinders, according to the experience of Europeana, the licensing of material protected under copyright law.

Thus, for legal reasons, Europeana neither includes versions of projects (about 90% of the books of the national libraries of Europe), nor orphan works (estimated at 10-20% of the collections protected under copyright law), which still protected under copyright, but the author cannot be identified.

According to the Communication of the European Commission from 19.10.2009 there are three important steps that should be taken:

1. Setting the right solutions for the legal consequences for digitization, especially those of the orphan works.

2. Working closely with the collecting societies and rightholders to clarify the legal complications in mass digitization and possible solutions to the issue of costs for rights clearance.

3. Finding practical solutions to facilitate rights clearance particularly through linking existing rights record in Europe (eg such as ARROW Accessible Registries of Rights Registration of Orphan Works towards Europeana).

A European digital library doubled its size, but there is no common European solution for online copyright.

Commissioner Reding, in charge of Information Society and Media, said: “Important digitization efforts have already started all around the globe. Europe should seize this opportunity to take the lead, and to ensure that books digitization takes place on the basis of European copyright law, and in full respect of Europe’s cultural diversity. Europe, with its rich cultural heritage, has most to offer and most

to win from books digitization. If we act swiftly, pro-competitive European solutions on books digitization may well be sooner operational than the solutions presently envisaged under the Google Books Settlement in the United States."

## References

Bottis M., The Google Library Project and copyrights of authors and publishers, TEKMIRION 2007, pp. 175-188 (in Greek).

Draft Report on "Europeana – the next steps" (2009/2158), 11/11/2009. Rapporteur: Helga Trueppel, Committee on Culture and Education, European Parliament

European Parliament resolution of 5May 2010 on "Europeana - the next steps" (2009/2158(INI))

Bearman, D. (December 2006). Jean-Noël Jeanneney's Critique of Google: Private Sector Book Digitization and Digital Library Policy, D-Lib Magazine, Volume 12 Number 12

Elhauge E., Why the Google Books Settlement is ProCompetitive, Winter 2010, Volume 2, Number 1, Journal of Legal Analysis

Ginsburg, J. C., Conflict of Laws in the Google Book Search: A View From Abroad, Columbia University School of Law, June 2, 2010

Grimmelmann, G., The ethical visions of copyright law, Fordham Law Review 2009, Vol. 77

Grimmelmann, G., The Amended Google Books Settlement is Still Exclusive, New York Law School Legal Studies, Research Paper Series 09/10

Grimmelmann, J. (2010), The Elephantine Google Books Settlement, online at: http://works.bepress.com/cgi/viewcontent.cgi?article=1031&context=james_grimmelmann /accessed 18.06.2010

Karakostas, I. (2003). Law and Internet: Legal Issues of the Internet, Athens, Sakkoulas.

Peritz, R.J. and Miller M. (2010), An Introduction to Competition Concerns in the Google Books Settlement, New York Law School Legal Studies

Renear, A. (1997). The Digital Library Research Agenda: What's Missing - and How Humanities Textbase Projects Can Help. D-Lib Magazine, July/August http://www.dlib.org/dlib/july97/07renear.html

Samuelson P. (2009), Legally Speaking: The Dead Souls of the Google Book Settlement, Forthcoming in 52 Communications of the ACM

Sinanidou, M. (2009). Informal publishing interactions: Linking, framing and meta-tagging in the book: Journalists and Publishers of Mass Media: Copyright Issues, (ed. Stamatoudi, I.), Thessaloniki, ed. Sakkoulas

Tenopir, C., & Ennis, L. (1998). The Digital Reference World of Academic Libraries. Online, Vol. 22, No. 4, available in: http://www.onlineinc.com/onlinemag/OL1998/tenopir7.html, accessed 18.06.2010.

# Electronic signatures in on-line transactions: legal issues in Greece and the European Union

**Christos Spyropoulos**

## Introduction

### *General approach*

Attempting to assess the impact of using electronic signatures while transacting on-line on the whole e-commerce regime that was created after the expansion of the Internet in the early '90s[1], what has to be initially estimated is the field of activities that such a way of signing covers. From a legal perspective, various parameters have to be taken into account, such as the contradiction between new techniques of trade with the traditional commerce and the special consequences that follow this fact-e.g. on-line/intangible v. paper-based contracts-, the universal nature of doing business via the Web with all the jurisdictional and applicability of law issues that arise automatically, the need of thje stablishment of a consumer-friendly system based on trust while striking a fair balance[2] between the companies' desire for success and the customers' request for protection against methods totally new to them and often used to take advantage of their "net-ignorance".

Problems like the above have become of great interest for the European Union's Member States as the economic integration in a Single Market where every european citizen will be free to move, work, provide services and buy goods is the ultimate purpose as set out in the EC Treaty[3]. Bearing in mind that Europe has always been struggling to create a more competitive market in comparison to the leading US market, the development of modern ways of trade seems to be essential to the former. Decisions, regulations, directives, are some of the weapons in the European Commission's arsenal that help in the process of harmonisation of standards between the Member States and guarantee a minimum legal framework on which special State legislation must be based.

Greece, as a Member State of the European Union located at a geographically crucial point (at the south-end of Europe and close to the emerging markets of the Balkan countries), has a dual role: on the one hand, it is obliged to adopt the European policy intiatives on e-commerce by implementing in a satisfactory extent the European Commission's directives and legislation in general, ensuring in that way its compliance with basic standards that warranty secutiry and progress;

on the other hand, although one could argue that e-commerce has no borders, Greece could play a leading role in the Balkans, a territory where it has traditionally been a key-player, in relation to electronic transactions by setting up a reputation of stability, secure trade and fair contracting policies.

Having referred, in general terms, to some controversial aspects of transacting on-line as well as to the milestone of the European Union's motivation when creating law and to Greece's twofold mission, we may assume that any attempt to legislate on electronic commerce has its origins in the first place at political (harmonisation, unification) and economic reasons (integration, creation of competitive markets based on consumer trust); the analysis of purely technical issues and their adaptation in a more comprehensible language through European or statutory legislation is a latter stage of action following the realisation of the need for legislative intervention.

## *The electronic commerce's notion*

Electrronic signatures are frequently used, inter alia[4], in the field of elecrtronic commerce as well as in the public administration system, in governmental organisations, in intelligent agencies e.t.c. The comprehension of the first presupposes the definition of the latter; as in the world of traditional trade the act of signing a paper-based contract from which obligations originate for both the contracting parties should be regarded as part of a set of legal rules that regulate the contracting procedure (imposition of rules of formality that guarantee the validity of certain categories of transactions-e.g. transactions on immovable things, last wills et.c.-v. absolute freedom of contracting-e.g. transactions on movable things-, designation of further rules that interpret the meaning/spirit of the law in cases of legislative gaps-e.g. in situations of modern ways of commercial activity that override the long-established ones, as often is the case in e-commerce-or formation of rules that solve problems arisen in special circumstances-e.g. fraud or use of threat while contracting), in the same sense signing electronically should be considered as a special facet of the entire on-line commercial practice.

Electronic commerce has habitually been defined as "doing business electronically"[5]; light is shed on this obscurely over-simplyfying and laconic description if we categorise the on-line commercial modus operandi, which is "based on the electronic processing and transmission of data, including text, sound and video"[6], in accrodance with two criteria, namely the type of the parties involved in it (businesses, governments, consumers) and the commercial activities covered by it (e.g. on-line delivery of digital content, on-line sourcing, direct consumer marketing, electronic share trading et.c.)[7]. Consequently, a number of transaction types is being shaped after the multiple combinations of the upper categories, such as the business-to-business (B2B) model which contains, for ex-

ample, the electronic trading of products and services, the business-to-consumer (B2C) model that encudes teleshopping, telebanking, electronic bookings (e.g. holiday or plane tickets), pay-TV or video-on-demand services, the consumer-to-consumer (C2C) model that includes virtual marketplace and electronic donation services, the administration-to-administration (A2A) model that refers, for instance, to electronic exchange of gorvernment information, the business-to-administration (B2A) model that is related, for example, to the electronic exchange of statistical information and the consumer-to-administration (C2A) model that embraces, for example, the provision of electronic tax forms services[8].

It becomes obvious that not only conventional methods of commerce which *prima facie* sound brand new (e.g. telebanking or virtual purchasing) are just the result of a successful adaptation of customary trading form the digittal environment with the help of modern technology, but also that traditional merchandising goes hand-by-hand with novel techniques seuch as web advertizing, electronic contract negotiation and electronic tax declarations. With the intention to prevent electronically transacting parties from acting in an anarchic way that would harm the e-commerce structure and, as a consequence, their own wellfare, the European Union has regulated certain aspects of on-line trade by adopting several measures such as the Directive on distance selling[9] and the Directive on e-commerce[10], both of which espouse a trading policy based on consumer trust, fair terms of trade and detailed description of rules and their exemptions. Being observed under the light of the above legislative spirit and the development of e-commerce as any transacting business activity related to the trade of goods or services between parties that "are not at the same physical location and communicate through electronic means"[11], the issue of electronic signatures could be analysed in a more comprehensive way.

## *The formation of electronic contracts' concept*

Under the "pre-Internet" legislation, a signature is used in transactions on several objects (e.g. purchase or rent of movable or immovable things or intellectual property rights); the common element of all the above deals is that persons who sign- either obliged by the law in order to breath life nd validity into their agreement/statement or after their free concurrence on being bound by a paper-based contract, in cases where the law is more flexible regarding formality matters-end up by confirming their will by signing at the and of a page or set of pages. The notion of the paper-based contract has been central in all these agreements which require that the wills of the parties must be drafted in a formally unambiguous way, as, Latins said, "*verba volent, scripta manent*". Therefore, signing has traditionally been relevant to paper-based deals and its task has been double, explicitly to verify the identity of the contracting parties and to confirm the fact that they

are willing to be bound by the content of the text as noted by them or a public authoriy or a legal expert.

The extended use of the Web as a means of doing business has brought into light a number of concerns far more complicated than the above formal requirements. Questions such as when are the on-line contracts formed, what terms they should include and which territory's law governs them[12] have become a case of study for legal and information technology connoisseurs. Using the method of functional equivalence as a starting point, these experts have tried to replace the function of long-established rules on contract law with modern ones compatible with the on-line merchandising[13]. Thus, for instance, considering the time when an electronic contract is shaped, a webvertisement is regarded as an invitation to treat[14] and not as an offer unless it unequivocally shows the keenness of the webvertiser to be bound upon acceptance[15]; in addition, the postal rule[16] applies to acceptances communicated through e-mail[17] due to the e-mail contracting procedure's similarity to the acceptance of a contract by post while the same rule does not apply to the click wrap acceptances[18]. Furthermore, considering the content of the terms a contract should include so as to be valid and not fall under consumer protection restrictions, it has been held that all contractual terms should be made known to the web client before he decides if he wants to enter in an agreement[19] and that the incorporation in the contract of terms by reference should be made in an explicit and definite way, e.g. by the provision of a "clearly marked and prominent link to the specific terms and conditions"[20], in order to help the customer shape a true choice on the purchase he intends to make. Moreover, in relation to which law is applicable to the contract, apart from the general principle of freedom of choice[21] that the parties have, special measures are taken when one of the parties is a "consumer", i.e. when his on-line purchasing is "outside his trade or profession"[22], namely that he cannot "be deprived of ... the protection afforded to him by the mandatory rules of the country in which he has his habitual residence"[23]. Accordingly, it becomes clear that the wisdom of the past which was gained through "trial and error" imposition of legislation or established case law is being repeatedly challenged by the rapid technological progress; thus, great effort and caution should be taken when implementing customary rules into the new way commerce is operating through the Net nowadays.

## *The electronic signatures' conception*

Regarding the electronic signatures as a special part of the above setting, the comprehension of their nature, functioning, mission and the problem caused during their use in the Internet environment becomes easier. Bearing in mind that a signature, either electronic or not, is meaningful only when connected with a contract or statement, and taking into consideration that electronic commerec is

a facet of a general policy or the European Union aiming at political and financial unification ane enforcement, the brief mentioning of some portions of e-signatures' analysis will be attempted below.

Starting by describing the variety of the ways of signing which exist traditionally or are being invented for electronic application, the way electronic signatures are functioning and the differences between habitual and modern techniques, the study will move on to examine the mission of signing in the contract world, to point out the several matters that are born while signing on-line and to scan the position which the European Union and Greece, in particular, have taken towards these vital issues. For instance, concerns on trust between the contracting parties are dealt with the creation of a "trusted third entity", namely the Certification Authority (CA) which guarantees the identity of the signatory; however, this model needs to be developed through specific legislation so as questions such as which body can qualify as a Certification Authority, who will decide on it, who will sypervise the CA's function, what sort of functioning levels-if any devision is permitted by law-will appear, what kind of measures will rule the liability of the Certification Authority towards its customer and the other contracting party, can be answered safely. In addition, the fact of the separation of electronic sugnatures into two types, that is to say in the "simple/conventional e-signature" and in the "advanced/qualified one" that is legislatively recognised as equal to the handwritten signature, will be observed from a consumer policy and Certification Authority improvement point of view.

The effectiveness of the e-signing methods like PKI (Public Key Infrastructure) cryptography in relation to data security will also be scrutinized, as the influence of an insecure on-line contracting regime on the potential market players' (consumers, businesses, governments) performance can be detrimental. The matter of key-escrowing will also be indicated as, by including by its very nature an offensive position against personal data protected by international[25], European[26] and national[27] legislation, it could create a negative conduct towards e-commercing. Finally, the measures protecting the consumers against on-line abuse of the existing legislation as well as the motivation given to companies to do business electronically will be commented in order to appreciate the extent to which a balance between consumer wellbeing and businesses' welfare is actually present and, if this is not the case, to propose some advanced solutions.

Focusing on Greece's activity relatively to the above, three views should be considered: firstly, that Greece is bound by having signed in several European Union agreements and, in that sense, obliged to follow up with the other Member States in the economic integration procedure. Secondly, that in order to achieve that purpose, Greece has to create law based on the European Direcrtive's on elec-

tronic signatures minimum legal framework by specifying the Directive's provisions which are the products of several influencies such as the Uncitral's Model Law on Electronic Signatures[28], the ABA's Digital Signature Guidelines[29] or Germany's Digital Signature Law[30]. Thirdly, that the adjustment of internationally standardised rules to the Greek legal system must comply with a number of social, cultural and economic needs of this State.

## Analysis

### *Traditional and modern signatures: sorts and legal definition*

Despite the fact that neither the European Directive 1999/93 nor the Greek Ministerial Decree 150/2001[31] that adopts the above Directive refer to the conventional or modern modes of signing in detail, probably because they take the existence of the former as self-evident and already sufficiently regulated by contract law and they prefer encouraging the development of new forms of e-signing than limitating it by recognising only a certain kind as legally valid for the latters[32], it is useful to denote them for two reasons: firstly, to understand how functional equivalence can be achieved for the benefit of e-commerce players and secondly, to appreciate how they are being treated by the law, and comprehend the reasoning for that treatment.

### *Signing formulae*

#### *Handwriting*

What traditionally has been regarded as a typical example of a handwritten signature is the writing of the name of the signatory at the bottom of the final page of the contract, deed or statement[33]. However, variant types have been created among the years, like crosses, initials, pseudonyms, identifying phrases, printed names or rubber stamps[34]. The clear resemblance which ties the above kinds is the fact that they are being transmitted, through the ink and the common knowledge of a particular alphabet, to a paper; nevertheless, in the absence of any intention of the signatory to sign and to be bound by any contractual obligations ("mental element"), his signature has no legal meaning[35]. Apart from the writing procedure and the medium on which they appear, the above signing models are alike due to the fact that they are the products of formality requirements set by the law; thus, their functionality is not examined in the first place[36].

*Modern applications*

On the other hand, the innovative trend of the technology is being reflected by the several ways of signing on-line. For reasons of completeness, what has to be clarified is the distinction between "electronic" and "digital" signatures. The first term is technologically neutral and covers the whole sum of techniques used for signing an electronic record[37]. The second covers electronic signatures created by the use of cryptography[38]. Some of the premature kinds of electronic signing have been the putting of the signatory's e-mail address under the document[39], the use of a secret code (PIN code) in debit/credit cards transactions through cash dispensers[40] or the "simple put of a name under an electronic mail"[41]. Moving ahead, we meet the biometrics technique which "uses physical or behavioural attributes such as your fingerprint, voice, face, iris or signature to identify you"[42]. Sorts of biometrics such as hand geometrics (scanning the shape or the size of the hand)[43], iris scanners (analysis "of the ring of the coloured muscle around the pupil")[44], facial (analysis of the video image or photograph of a person) or vocal (analysis of "fundamental voice characteristics") recognition[45] and signing characteristics' recognition (examination of "the speed and acceleration rates of the pen strokes used to make the signature" on a special equipment called "digitising pad")[46] are frequently used by governments and companies to increase security in on-line transactions. Steganography, the science of "hiding secret data inside a common filer type so nobody guesses that it is there"[47], applies to "secret messages written in invisible ink, micro dots and radio signals that resemble noisy static"[48] and is regarded as a great threat for on-line security if used by extremists or terrorists[49]. Furthermore, quantum cryptography refers to messages being sent by the use of photons of different polarities that represent numbers (zeros or ones)[50] and is expected to be the safest way of on-line communication in the near future, although the fears of being attacked are always present[51].

*Cryptography*

Cryptography is the most widespread technique of electronic signing. The term originates from Greek ("crypto" means secret + "grapho" means write) and encapsulates the idea of hiding the meaning of a message by writing it in another way known only to the receiver of it.[52] The above purpose is met by the enciphering of the message by the sender and its deciphering by the receiver, which in turn is attained through the use of algorithms, i.e. arithmetical processes that encode data based on mathematical calculations. In order for the message to be signed and read, both its creator and its recipient have to possess keys, in a metaphorical sense: each of them has a public key known to the other and a private key that is kept secret. Hence, two pairs of keys are needed for the encoding and decoding

of the message, and this is the example of assymetrical or public key cryptography[53]. In symmetrical or private key cryptography, there is only one "private" key which the parties share to encode and decode and which they agree to keep secret[54]; thus, the level of confidentiality and trust between the parties has to be remarkably high and symmetrical cryptography applies to closed networks, i.e. networks with limited participants such as pay-TV, pay-per-view or video-on-demand services[55]. The open-networked nature of the Internet and the fundamental element of secure and safe web-transacting have made public key cryptography the common method for the formation of electronic signatures[56].

As mentioned above, public key cryptography is based on "the technology of sharing a public key"[57]. The comprehension of its functioning could contribute in understanding a number of legal issues such as the Certification Authorities' mission towards the consumers and the governments in the course of on-line trade. Considering A as the composer and sender of an electronic message and B as the receiver of that message, the following process takes place: (i) by applying an algorithm called "digest" or "hash function"[58] to the written message, A transforms the original text into a string of bits which is unique and brief and is called the "message digest", (ii) in order to make the message digest secret to any other accidental receiver or hacker, A encrypts it with his private key[59]; in particular, A performs a series of mathematical procedures between the digest and the private key, and the result is a number that forms the electronic signature[60]. A can additionally encrypt his message with B's public key for extra security, (iii) in order to decrypt the message, i.e. to bring the sent message in plaintext form again, B will use A's public key; decoding will fail if someone else used A's public key but his own private key to sign the message. Furthermore, if A has encrypted the message using additionally B's public key, B will have to decrypt it using his private key; in that way, A can be sure that only B-or persons authorised by B to know and use his private key will read his message, (iv) the plaintext message is run through the same algorithm (hash function) and a message digest is produced, (v) B compares the message digest of the sent and the recieved messages; if they differ, even in one bit, the sent message has been altered in transit[61]. If they are the same, A's signature is validated and the integrity of the plaintext is guaranteed.

## *European and greek legal definition*

### *The European approach*

Regarding signing as a common phenomenon among the centuries, it seems futile trying to find a definition in European legal texts; the national laws of the Member States are a better object of examination. However, the concept of electronic signatures, due to its rather complicated and technical character in comparison to

handwritten signing and to its significance for the augmentation of e-commerce, has become of great interest to the European legislative world.

The European Directive 1999/93 on Electronic Signatures defines an electronic signature as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication" [art. 2 (1)][62]. This quite broad definition is justified by recital 8 of the Directive, which says that due to the speedy progress of technology and the worldwide nature of the Internet, every legislative approach on electronic signatures has to be 'open to various technologies and services capable of authenticating data electronically", i.e. technologically neutral[63]. The technological neutrality principle is also met in art. 2 (4) and art. 2 (7) of the Directive, where, although public or private key cryptography are recognised as methods of creating and verifying an electronic signature, the use of "such as" indicates the European Union's desire to leave the doors open for innovation, research and development.

The novel notion that the Directive embraces is the two-tier approach[64] it adopts in relation to the legal recognition of electronic signatures. In particular, it provides for two types of electronic signatures, namely the "simple" and the "advanced" electronic signature. The first is defined in art. 2 (1), the latter is an advanced version of the first and is defined in art. 2 (2) as "an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory, (b) it is capable of identifying the signatory, (c) it is created using means that the signatory can maintain under his sole control and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable"[65].

*The Greek approach*

The greek contract law does not give any definition of the term "signature"[66]. Nonetheless, art. 160 para 1 of the Civil Code states that, in the case that a document is required by the law[67] or agreed by the parties to be in written form, this document will be regarded as valid only if it carries the handwritten signatures of the parties[68]. Inspite of being necessary for reasons of contracts' security and confidentiality, the above provision proves to be strictly formalistic as it calls for signature written in hand[69], even though Greek case law has broadened the horizon of hand-writting by recognising as legal valid signtures put by foot or mouth or signatures created by technical means such as fax or telex. In addition, it is indirectly incosistent with art. 444 (3) of the Civil Procedure Code, as the latter, in the course of the evidential procedure, defines "document" as "any mechanical pictuation" and allows, in that way, techniques such as video or tape recordings or-in a further extent, electronic mails- to be legally accepted. The gap that appears in the case e.g. of an e-mail contract is noticeable, as signing the e-mail can-

not be made by hand but only by using electronic means, which, in turn, must be recognisable by law (broader interpretation of art. 160 para 1 of the Civil Code) in order for the e-mail document to be accepted as evidence and legally binding the parties. The only solution that prima facie seems feasible is the consideration of the several manners of e-signing as equal in nature to the legally admissible traditional hand-signing ways, for reasons of development of e-commerce and support of the technological growth[70].

With reference to electronic signatures, the Ministerial Decree 150/2001 which has adopted the European Directive 1999/93 gives exactly the same definition of art. 2 (1) and art. 2 (2) of the Directive for the electronic signature and the advanced electronic signature respectively in its art. 2 (1) and 2 (2). The same technology neutral spirit also appears in art. 2 (4) and 2(7)[71]. It is evident that the Greek legislator wishes to avoid any deviation from the European letter and spirit of the law so as to contribute in the harmonisation process and the expansion of e-commerce in Europe by adopting in the larger extent the European Commission's policy dicta. It is also beneficial for Greece to bring its legislation on e-commerce into line with the European standards from an early point in order to avoid s "follow-up" tactic later that could harm its national status[72]. Furthermore, the creation of a secure regime for on-line trading could make Greece a crucial player in Balkan's economic life.

As a consequence, two parameters have to be kept in mind: firstly, the construction of a double-typed model for electronic signatures by the European Directive and its adoption by the Greek law and secondly, the European Commission's willingness to support the appearance of new technologies on e-signing by defining electronic signatures in such a broad way[73]- provided that the safety requirement is satisfied and improved by pioneering methods which suit to the Directive's security standards[74]. The examination of the handwrittem and on-line signatures' tasks as well as a comparison between those two categories will take place below.

### *Signatures' mission*

The comprehension of a signature's purpose is the starting point for the understanding of its legal meaning and the realisation of the problems its use may cause in the electronic environment. Invented to satisfy the security and reliability requirements for safe transacting, a signature fulfills four tasks[75].

### Authentication

By signing at the last page of a paper-based contract or by applying the essential mathematical procedures to decrypt an electronic message, the signatory not only indicates his intention to identify himself as the originator of the text but also sugnifies his purpose to be legally bound by the content of that text. Thus, the

primary role of a signature is to identify "who participated in the transaction"[76]. The authenticity of the signature is the result of a successfull decryption procedure as discussed above which, apart from the case where the signatory has lost control of his key by accident or purposively[77], provides the verifying party with the information that the party that signed the message electronically is the same person who possesses the public key which the verifying party used to decrypt the message.

The authentication part of e-signatures is regarded as an element of their definition by Directive 1999/93, as in art. 2 (1) e-signatures are defined as "data... which serve as a method of authentication"[78]. The Greek Ministerial Decree 150/2001 fully accepts the importance of the authentication aspect by implementing in art. 2 (1) the Directive's art. 2 (1) word for word.

## Data integrity

What follows the question on the identity of the signatory is the matter of the veracity of the message's terms[79]. It is of great importance for the receiver of a data message[80] (e.g. en e-mail taken as an offer for contracting) to be reassured that what he reads after having decoded the message digest is what the signatory intented to communicate to him without the data having been modified, demolished or accessed by any unauthorised person. The integrity of the data contained in the electronic message is being proven at the same time with the authenticity of the electronic signature[81], namely after the realisation of the fact that the message digest of the sent and the received message is the same. The issue of integrity is critical not only for the consumers (B2C commerce) as, for example, consumer protection concerns are born by the alteration of on-line contractual terms and conditions without the authorisation of the on-line company (e.g. by a hacker of an antagonistic company) and the consumer's prior notification, but also for the business (B2B commerce) as, for instance, orders between companies that occur daily on-line could be declared void in the absence of consistency between the sent and the received offer. Subsequently, the whole structure of on-line trading would be collapsing if not based on a method of e-signing that would promote security and safety, i.e. PKI encryption.

The European Commission, acknowledging these perils, although, as mentioned above[82], it does not establish PKI as the exclusively superior technology, it refers in the Directive to "signature-creation data" (e.g. codes or cryptographic keys) "used by the signatory to create an electronic signature"[83] implemented by "signature creation device" ("configured software or hardware")[84] or "secure-signature-creation-device"[85] and to "signature-verification-data"[86] (e.g. codes or public cryptographic keys) used to verify an electronic signature which are implemented by "signature-verification device" ("configured software or hardware")[87].

It becomes plain that the regulation of such a technical matter like e-signing in a pan-European level, in combination with the imperative need for a comprehensible legal text which will guarantee stability and progress in the European Single Market, has to take into serious consideration the technological background as well as the new electronic signature products[88]. The Greek Ministerial Decree 150/2001 entirely implements the above provisions in its art. 2 (4)-(8).

## Confidentiality

The concept of confidentiality is based on the idea that any commercial transaction (e.g. commercial negotiations on the formation of a contract, offers and acceptances e.t.c.) carried out through the Web should be readable only by the contracting parties. This can be achieved only if each of the parties has complete control over his private key; it can be strengthened if the signatory encrypts his message not only with his private key, but also with the receiver's public key, so that only the receiver can read the message by decrypting it using his private key. Regarding the encryption algorithm as the lock of a safe and the private key as the combination to open that lock, we can understand that, as a multi-numbered combination makes the lock less vulnerable to theft, in the same way a lengthy private key protects the algorithm against attacks and, thus, the message against unauthorised access[89]. A technical example is this of the pay-TV services, to which only users under a contract have access; this is being achieved by the provision to the user of the necessary equipment (hardware, software, interfaces) so as to be able to decrypt the programme that is being broadcast with the use of his set-top box[90].

Confidentiality comes as a physical consequence of the confirmation of the fact that the signatories are the ones that they claim to be (authentication) and that the content of the data message has not been altered (data integrity). Directive 1999/93 does not refer explicitly to the notion of confidentiality, probably because the satisfaction of the authentication need through the use of advanced technology is regarded as automatically covering the requirement of secrecy. However, recital 6 inserts a problematic perception when it says that "This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security". It is obvious that the European Commission not only is unwilling to take a position towards the key-escrow issue[91], but also creates, with such a neutral approach, the potential for the governmental intelligence agencies to abuse any individual's privacy while he is contracting on-line for reasons of national security or public policy/safety. art. 8 of the Directive comes as a panacea, as it imposes on the Certification Authorities the obligation to comply with the Data Protection Directive 2002/58/EC[92]. In addition, the re-

cital 18 of the Directive says that "the storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures". However, the Directive seems to leave the possession or controlling of private keys directly from the government unregulated. The Greek approach is identical, i.e. confidentiality is taken as self-evident when authentication is fulfilled; art. 7 (1) and (2) of the Ministerial Decree deals with data protection matters by putting Certification Authorities under the "sword of Damocles" of Greek laws 2472/1997 and 2774/1999 on the protection of individuals from processing of personal data.

## Non-repudiation

The fourth mission of a signature is to prevent the signatory from denying that he made and signed a particular statement[93]. Non-repudiation follows the previous principles of authentication, data integrity and confidentiality. As long as the identity of the parties, the truth of the message's content and the secrecy of it have been verified, none of the signatories could refuse to be legally bound by the terms of the message/contract[94]. Non-repudiation can be divided into "non-repudiation of origin" which prevents the creator of the messaage from claiming that he did not send it, and "non-repudiation of delivery" which prevents the message's receiver from denying having received it. Additionally, a distinction between "non-repudiation of enforceability" and "non-repudiation of authentication" has to be made[95]: the first refers to situations such as when signing was "procured by duress or fraud, if it was based on a material mistake of fact" e.t.c.; in such cases, no matter how reliable is the signature-creation and verification device, the hypothetical contract lacks of enforceability due to circumstances that have taken place outside the verification technique's detectability. The second refers purely to the technical procedure of authenticating a signature and the data integrity of a message; in that case, the signatories are bound by the on-line contracting game they themselves have chosen to play and, as a result, no denial of the validity terms is acceptable by the court.

It becomes obvious that non-repudiation is a matter that arises in the case of a dispute over the validity of a signature and the acceptance of the terms of a contract. Yet, Directive 1999/93 takes a controversial position on the matter: although it declares in recital 17 and in art. 1 that "it does not cover aspects related to the conclusion and validity of contracts or other legal obligations... nor does it affect rules and limits...governing the use of documents"[96], it provides for advanced electronic signatures to be "admissible as evidence in legal proceedings"[97]. The hypothetical example of an on-line contract, whose validity, although it has been signed with the advanced electronic signatures of both parties, is being challenged by one of them on the basis of threat, raises the dilemma:

"is the judge obliged to rely on the 100% assurance about the authenticity of the electronic signature whcih the verification procedure guarantees or does he has to apply the traditional rules of contract law on fraud or duress while contracting"?

In my opinion, by making advanced electronic signatures equivalent to handwritten signatures when it comes to evidential matters, the Directive does not (or should not) support the idea that a verified advanced e-signature can guarantee both for the technical genuineness of the message's content and the authenticity of the signatory's will. As long as on-line trading is being operated between human beings through computers and not merely between computers, the human factor has to be taken into account when validity of will is disputed. Thus, the judge in the above example will just consider the advanced signature as valid[98]; it is a matter of proof if finally a threat is proved to have taken place and a matter for Greek contract law or law or evidence to set a special rule which will provide for a combining solution. In addition, recital 21 of the Directive says that "...this Directive...does not affect national rules regarding the unfettered judicial consideration of evidence.

## Concluding notes

What becomes clear from the above analysis is the quadraple mission of traditional and, more importantly, electronic signatures. The identification of the contracting parties[99], the integrity of the data content of the message[100], the guarantee that the encrypted message has not been accessed, altered or devastated[101] ("time-stamping services" and "computing services" are encouraged by the Directive in recital 9) and the prevention of the signatory from denying "having performed a particular action related to data"[102], i.e. from disclaiming that he meant to sign and send the message to the receiver, shape the meaning of e-signatures' existence. The European Union concedes that, in order to construct a stable and progressive e-commerce regime, it has to apply the new technologies to its legislation if high levels of security are guaranteed. For that reason, terms such as "signature-verification-data" or "secure-signature-creation-device" appear on the Directive without being furtherly specified as long as they comply with a basic level of ability to provide security. The Greek law loyally implements the Directive's provisions trying to act in accordance with the European policy on law harmonisation and financial unification.

Manuscript and electronic signatures are aiming at fulfilling the same tasks. Firstly, they indicate the signatory's intention to be regarded as the author of the document and as the person that deliberately incorporated his ideas in that document in order to be legally bound by its content. Secondly, they guarantee the integrity of the terms included in the document; this is the reasoning of the obligation according to which the signatory of a contract has to sign in every single

page of his will. In electronic documents, this is pledged by the application of public key encryption. Thirdly, the secrecy of the information contained in the document and the non-repudiatibility of its content come as a normal result of its previously verified authenticity.

However, there are differences in some aspects. For instance, a handwritten signature is "in the flesh" connected with a carrier[103], i.e. the paper page, a fact that makes it automatically readable and tangible and, thus, more detectable about its authenticity. On the other hand, due to the metaphysical nature of the electronic document[104] (though visible, it is not touchable, and what we see is just Os and 1s on the screen of our computer), any alteration on it is hardly measurable and, thus, advanced technology such as biometrics, time-stamping or watermarking is needed to increase security. In addition, an individual's manuscript signature is unique due to every person's inimitable handwriting[105] and thus difficult to be completely copied, and when this happens, graphology specialists often uncover the forgery. In contrast, because of the fact that an electronic signature is based on the concept of the possession of a private key that has to be kept secret[106], it is extremely easy for any person that may attain access to the private key[107] to represent himself as the signatory and transact on the latter' s behalf without his knowledge and consent.

Judging by the similarities and differences between handwitten and electronic signatures, and despite the fact that the technological nature of the latter makes them seem so complex and diverse from the firsts, we should not focus on trying to find out which of these triumphs over the other. Rather, we should examine how they can function in combination for the development of e-commerce.[108] This is the approach that the European Union, and consequently Greece, has taken. In particular, art. 5 (1) (a) of the Directive 1999/93 equalises the legal effectiveness of an electronic signature[109] to this of a handwritten signature; obviously, the Directive attempts to treat advanced security signatures in the same manner with the handwritten ones, indicating in this way two ideas, i.e. that it is unwilling to establish a completely new and exclusive regime for electronic signatures[110] and that it acknowledges the quantitative and historical prevalence of traditional signing over on-line signing (for reasons of consumer confidence[111]). Based on the priciple of functional equivalence which represents the idea that legal admissibility should be given to electronic signatures if the way of their creation provides the same degree of security and authenticity as the handwritten signing, art. 5 of the Directive "reconciliates" the two signing categories.

The Ministerial Decree 150/2001 fully adopts the above approach; from a case law point of view, Decision 1327/2001 of the One-Member District Court of Athens[112] reaches to some interesting conclusions. In particular, in the text of

the decision it is said that although the electronic document, due to the lack of its stability and lifetime durability when being incorporated in a hard disc, can not be regarded as much alike to the traditional document, it can be considered as legally equal to the latter. The Decision describes that an e-mail address, due to its uniqueness and creation by the e-mail sender by himself, "has the character of a handwritten signature, independently of its position on the electronic document" and is admissible as evidence in legal proceedings. The judge bases the legal effect of the e-mail as a handwritten signature on the fact that, due to common experience, the creation of the e-mail presupposes a server connected on the Internet through a software installed in the owner's computer and a special code through which the owner of the e-mail is being uniquilly recognised as the sender or the receiver of electronic data. The above code is created originally by the owner and consists of characters (numbers, symbols, letters et.c.) selected by him which, connected with the symbol @ and characters set by the server, form the e-mail. In that sense, the Greek judge concluded that the authentication and the non-repudiation of the e-mail signature was undoubted. The eagerness of the Greek judge to validate electronic contracts and, thus, create a friendly environment for the growth of e-commerce is obvious. However, from an electronic signatures' authentication point of view, the judge has misunderstood two aspects: firstly, that the security provided by the method of creating an e-mail address does not meet the standards imposed by the Directive 1999/93 [advanced electronic signature created by a secure-signature-creation device, art. 5 (1)][113]; secondly, that the existence or not of a qualified certificate that would guarantee the true connection between the owner of the e-mail address and the sender of the e-mail document and would make the e-mail address equal to a handwitten one according to art. 5 (1) of the Directive was not examined.[114] Taking into account that the concluded via e-mail contract was worth approximately 25.000 fr relatively large amount of money- and that most of the Certification Authorities (CAs) classify the signature certificates they provide in accordance with each transaction's value[115], the acceptance of the effectiveness of the e-mail address as an electronic signature equal to manuscript signature seems overenthusiastic if compared to the security requirements for on-line dealing.

In the Decision 3279/2004 of the Council of State, the Greek judges had to deal with a slightly different situation: the chinese company that submitted its offer to the Ministry of Public Constructions did not meet the requirements of the greek Ministerial Decree for public contracts. More specifically, the company's papers had only the company's electronic seal and not the handwritten signature of its legal representative as the Greek law for public contracts demanded for reasons of public order and safety. This fact created serious doubts to the judges on the authentication of the electronic seal and the true will of the company to be bound

by the contract in case that someone else had become in possession of the seal. In other words, the Decision used the aspect of public order and common good which the Ministerial Decree had set as a legal prerequisite for the legal recognition of any type of signature on electronic papers and put a limit on the general acceptance of unclassified signatures, though without examining the field of signature's digital formation and its legal aspects.

In Decision 25208/2009 of the One-Member District Court of Thessaloniki, the judge faced another common problem: considering the e-mail address of a woman as her electronic signature, he concluded that the "breaking" of its password by a third person and the sending of e-mails to other people without her consent was, apart from an offence to her personality, a forgery of her "electronic signature" as well.

Therefore, handwritten and electronic signatures can go hand-by-hand, provided that full respect is being attributed to the risks resulting from the false application of novel technologies while, at the same time, the structure of the existing legal system (contract law, law of evidence) is accepted as the basis for every legislative work on e-signing.

## *The Trusted Third Party's concept*

### The necessity for Certification Service Providers (CSPs): On the Internet, nobody knows you're a dogl[116]

Due to the dematerialisation of transactions on the Web world[117], physical contact between the agreeing parties has been flattened. Thus, while in traditional trade it is usual that the signatories of a contract know each other, either personally or through their lawyers, in on-line contracting the parties often transact for the first (and last) time. The issue of knowing who really the other party with which we deal electronically is, is fundamental for the establishment of trust in e-commerce. The procedure of the verification of the authenticity of an electronic signature based on PKI encryption solely assures the recipient of the electronic message that the person who theoritically possesses a public key is the one that sent the message[118]; however, it does not answer to the following questions:

a) is the possessor of the public key the person that he claims to be, i.e. is there a real connection between phenomenical and actual identity of the signatory?

b) regardless of answering positively to the above question, was the signatory in real possession of his private key or this had been lost or stolen at the time of the transaction?

From a personalisation point of view, the problem is that the private and public keys form a pair of numbers that has no relationship with the actual identity of a

person[119] as it does not attibute to him some special characteristics (e.g. height, date of birth etc) which his identity card contains. Therefore, it is possible and trouble-free for a third party to create a pair of keys, place the public key in an on-line directory under somebody else's name and begin signing electronic messages in this else's name[120]. As a consequence, what the transacting parties struggle for is the affirmation that each others' public keys truly belong to whom it is claimed. The identity problem refers to transactions in open networks like the Internet where the parties have not established a previous commercial relationship[121] and the demand for trustworthiness is imperative. The notion of Certification Authorities (CAs) or Trusted Third Parties (TTP) or Certification Service Providers (CSPs) appears in order to serve the above purpose, namely to warranty the relationship between the identity of the signatory and his public key.

## CSPs' mission

Having understood the underlying reasoning for the existence of CSPs, it is unadorned to define their mission. A CSP declares to ascertain the identity of a signing party and certifies that this party's public key in fact belongs to him.[122] Thus, the linkage of signature verification data (e.g. codes or public keys) to a person and the confirmation of that person's identity[123] is the motivation of the CSP's function with the eventual purpose of intensifying confidence in the e-commerce scenery.

## Designation of CSPs

By its definition, a CSP plays the role of an entity that acts as an intermediary [124] between the contracting parties as it satisfies the request of the one (receiver of the signed electronic document) to know the identity of the other (sender of the message). In other words, a CSP aims at being trusted by the receiver in relation to the accuracy and completeness of information it provides him about its customer (the sender). To achieve this reliability in the receiver's mind, the CSP must be designated as an independent unit.

Directive 1999/93 defines broadly a CSP as "an entity or a legal or natural person" [art. 2 (1)]; the Ministerial Decree 150/2001 defines a CSP in exactly the same way [art. 2 {11}]. The Directive leaves the structure of the CSPs (and the services they may provide) to the legislators of the Member States according to recital 12 and art. 4 (1), with the sole restriction of art. 3 (1)[125]. The Ministerial Decree declares that the provision of certification services in Greece by a CSP that is established in the Greek territory is ruled by the existing Greek legislation [art. 5 (1)]. In relation to the above restriction, the Decree states in art. 4 (4) that, apart from art. 4 (5) (provision of voluntary accreditation by the EETT[126]-or private or public bodies authorised by EETT-after the submission of a written ap-

plication of the interested party) which complies with art. 3 (2) of the Directive, the provision of any form of certification services in Greece is not dependent on a license given to the CSP.

Among the different forms of structure, such as a state-controlled entity[127], a mainly owned by the government private legal person[128] or an entirely independent corporation, the Greek practice has selected the third model to incorporate the idea of CSPs. Thus, at the moment, nine CSPs are active in Greece according to the data archive of EETT[129]: two of them are bank entities, another one is "an obligatory, autonomous and independent association of natural and legal persons, conducting commercial activity in a given region, and operates under the constraining administrative supervision of the Minister (with respect to the legality of its activities within the context of its statutory autonomy)"[130] and the other four are governmental organisations or private entities. Only three of them (www.ase.gr, www.ypesdda.gov.gr and www.adacom.com) provide their customers with a certificate that complies with the Directive's definition of a"qualified certificate".[131]

In a further extent, and in order to fill in the potential gaps regarding the designation of CSPs, the European Commission has adopted Decision 2000/709/EC[132] "on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3 (4) of the Directive 1999/93/EC ... ". art. 3 (4) of the Directive refers to public or private bodies designated by the Member States and having the responsibility to determine "the conformity of secure signature-creation devices with the requirements laid down in Annex ΙΙΙ». The purpose of Decision 2000/709 is to establish the legal framework on the requirements such a body should fulfil in order to be designated as responsible for the above task. Thus, the independence aspect of that body will be covered if its stuff is not engaged in designing, manufacturing, supplying or installing of secure-signature-creation-devices or in providing CSPs services and if the body is financially independent (art. 3). The body' s personnel must carry out its task with "sufficient technical competence" (art. 4) gained by "sound technical and vocational training" [art. 7 (1)] and "satisfactory knowledge and ... adequate experience" [art. 7 (2)]. The impartiality of the staff (art. 8) as well as the adequacy of the financial sources of the body "to cover liabilities arising from its activities" and the sufficiency of ways "to ensure the confidentiality of the information obtained in carrying out its tasks" (art. l0) are also of great importance.

The Greek response to this Decision is incorporated in the Ministerial Decree's provisions. In particular, EETT-"an independent self-funding decisionmaking body"- has the responsibility: (a) to examine the compliance of any secure-signature-creation device with the provisions of Annex ΙΙΙ of the Directive and

the Decree [art. 4 (2)), (b) to provide voluntary accreditation to any interested party that complies with specific security standards, (c) to supervise all the CSPs that are established in Greece and (d) to inform the European Commission about the names and the addresses of all the accredited CSPs in Greece. In addition, EETT has already come up with "the criteria for the selection of Designated Bodies (in either the public or private sector) for ascertaining compliance with secure-signature-creation devices".[133] This statement could be interpreted as an attempt of the EETT to decentralize the task of confirming the compliance of CSPs with specific security standards preventing in that sense the monopolisation of such a responsibility by one authority and reinforcing competition (i) between the potential confirming bodies, by giving them motivation to operate in the most appropriate way and (ii) between the latent CSPs by demanding the best functioning that will satisfy the same minimum but different additional criteria settled by the various confirming bodies; the final purpose remains the benefit of the consumers and businesses dealing in a secure weboutlook.

## Functioning of CSPs

### *Issuance of certificates and other services*

The satisfaction of the requirement for trust is met not only by the proper designation of the CSP as an independent body but also by its appropriate functioning. The European Commission adopts that notion in two ways. Firstly, by defining the issuance of certificates or the provision of "other services related to electronic signatures"[134] as *the* main duty of a CSP, in combination with recital 9 (definition of products and services related to electronic signatures not limited to "the issuance and management of certificates" but also encompassing "any other service and product ... such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures"), the Directive allows a CSP to function in a variety of technical applications. Thus, for instance, it can generate the private and public key of its customer, register the identity and examine the official documents of him, revoke public key certificates, provide time stamps on certificates or govern directories of public key holders.[135] The aim of the European Union is palpable, namely to hearten the creation of advanced and multiple technologies and to ensure safety and security in on-line transactions.

### *Provision of (simple) and "qualified» certificates*

The Directive provides for two sorts of electronic signatures' certificates, that is to say the (simple) certificate ["an electronic attestation which links signature-verification data to a person and confirms the identity of that person", art. 2 (9)] and the "qualified certificate" ["a certificate which meets the requirements laid

down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II», art. 2 (10)]. This categorisation, though *prima facie* theoritical, has practical consequences because art. 5 (1) depends the legal effectiveness of an advanced electronic signature on it is being based on a qualified certificate. Thus, the admissibility of an advanced e-signature as evidence in legal proceedings and its equality with the handwritten one highly depends on the fact that it can be verified through a qualified certificate; it is clear that the whole tendency of recognising electronic signatures as equal to manusript relies on the satisfaction of the requirements of Annexes I and Π of the Directive and of the Ministerial Decree.

Annex I asserts a compulsory list (ten conditions) of the content of a qualified certificate. The name of the signatory or his pseudonym (cond. c), the indication of the beginning and end of the period of validity of the certificate (cond. f), the advanced electronic signature of the certification-service-provider issuing it (cond. h) and any limitations on the scope of use (cond. i) or the value of transactions for which the certificate can be used (cond. j) are some of the elements that must be contained in a qualified certificate. Annex I of the MinisteńaI Decree implements the above list literally.

Annex II contains a list of twelve prerequisites which must be fulfilled by a CSP when he issues qualified certificates. The operation of a "prompt and secure directory and ... revocation service" (cond. b), the ensurance that "the date and time when a certificate is issued or revoked can be determined precisely" (cond. c), the verification of the identity and of any "specific attributes of the person to which a qualified certificate is issued" (cond. d), the employment of experienced personnel (cond. e), the adoption of reliable measures against forgery (cond. g) and the non-storage of signature-creation data (private keys) of the person to whom the CSP provided key management services (cond. j) are some of the mandatory rules a CSP issuing qualified certificates must obey. Again, the Decree entirely adopts the above provisions in its Annex Π.

The above brief reference to Annexes I and II signifies the intention of the Directive to construct a technologically welcoming field for e-commerce based on trust. To achieve this, it has to accept models of electronic signatures that are simple and certificates that guarantee for these signatures that are simple too. It also has to encourage the adoption of advanced e-signatures and qualified certificates. This two-stage process is not only unavoidable but also necessary in this early period of e-signing. By showing its preference to advanced signatuers and qualified certificates, the European Union indirectly declares to the Member States and to any CSP willing to provide products and services that, although in theory even an e-mail address can serve as electronic signature, practically in the near future

what will be safer and convenient for the on-line consumers and businesses for the sake of trust is the sophisticated technology and its applications such as the advanced electronic signature and the quaIified certificate. Thus, it succeeds in not discouraging the average consumer from doing business on-line while, at the same time, it encourages the operation of safer e-commerce. A practical example of this attempt is art. 5 (2) of the Directive, which imposes on Member States the obligation to ensure that solely being in electronic form or not being advanced or not being quaranteed by a qualified certificate issued by an accredited certification-service-provider does not suffice foι an electronic signature to be "denied legal effectiveness and admissibility as evidence in legal proceedings". There must exist other reasons, based on legal defects (e.g. proof of use of threat during the transaction) or factuaI deficiencies (e.g. proof of existence of non-reliable personell of the CSP) that will permit the judge not to admit the electronic signature as evidence.

*Voluntary accreditation of CSPs*

For reasons of enrichment of the electronic signature products and services' market, for a CSP to provide certification services it is not necessary to gain prior authorisation[136] from a govemmental organisation, a public authority, a private legal person or a natural person. However, the European Union is aware of the dangers a totally lawless market access regime can enfold. Therefore, recital 11 of the Directive states that the purpose of voluntary accreditation schemes is the stipulation of an "enhanced Ievel of service-provision [by the CSPs]" and the "development of best practice among certification-service-providers" by offering them "the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market". The national law of each Member State shall additionally ensure the freedom of the CSPs to operate outside or inside voluntary accreditation schemes (recital 12), to remain and to make profit from such schemes (recital 11). Moreover, no discrimination (e.g. by the courts or the public administrative authorities) between accredited and non-accredited CSPs should exist, as this could be injurious for the level of competition between them (recital 12).

For those CSPs that have chosen to be accredited, art. 3 (2) provides that the preconditions for a successful accreditation should be "Objective, transparent, proportionate and non-discriminatory"; additionally, there is no *numerus clausus* i.e. 1imited number of CSPs that are allowed to be accredited, provided that their functioning falls within the scope of the Directive. The idea from which the voluntary accreditation notion originates is that the participating CSPs in such a scheme will compete with each other, firstly so as to comply with the requirements of the scheme, and secondly to gain the largest share in the market of cer-

tification services provision. The subsequent benefit for the net-consumers will be manifest as they will enjoy high quality technological services[137]. It is also suggested that the voluntary nature of the scheme makes it more flexible than a mandatory model because the participating CSPs' welfare will attract those operating outside to invest and innovate and finally enter the scheme for the benefit of trust.[138]

The operation of voluntary accreditation schemes has been spread throughout Europe. For example, to Scheme in the UK is an "independent, non-profit making industry led body" established to guarantee that CSPs' services are provided "honestly and expertly" and ensure confidence between CSPs and consumers. By providing the CSP' s web page with a "web seal" which acts as a trust mark, tScheme reassures the consumer of a CSP that the latter has been independently examined by experts and meets high level security standards, that it complies with a specific "code of conduct" and that it will "act promptly and fairly to remedy faults"[139] In Greece, although art. 4 (5) of the Ministerial Decree provides for the institution of voluntary accreditation schemes, EETT has not yet formed a specific scheme[140]. Finally, what has to be clarified is that the participation in such a scheme is not obligatory for the provision of any certification services ('simple' or 'qualified' certificates); the purpose which such an option serves is the organisation of CSPs in a group that will provide high quality services for the benefit of consumers. However, it is likely in the near future that the partaking in such schemes will be the only alternative for a CSP that will aim at gaining a considerable market share in CSPs services' field.

## Supervision of CSPs

Art. 3 (3) of the Directive obliges each Member State to establish an appropriate system for the supervision of CSPs located on its territory and providing qualified certificates to the public. Apart from the fact that this paragraph refers exclusively to the CSPs that issue qualified certificates and leaves, in that sense, the activity of the rest unregulated, what is more important is its contradiction with art. 3 (1) which prohibits the prior authorisation (or "any other measures having the same effect", recital 10) as a prerequisite for the provision of certification services. And if we consider the importance of a qualified certificate for the legal status and admissibility of an advanced electronic signature [art. 5 (1)], the proper supervision of the provider of such a certificate is of crucial significance for the whole functioning of e-commerce.

Art. 3 (3) leaves it to the national laws of the Member States to find the best formula for striking a fair balance between the need of the consumers for trustworthiness and the craving of CSPs for freedom of electronic signatures' services flow. Trying to avoid the notion of prior authorisation, some Member States have come

up with the idea of giving "notification to the appropriate public authority before starting the provision of services".[141] However, notification can be regarded as a measure having very similar effect with prior authorisation and it will remain to the national and European courts to judge on the correct implementation of art. 3 (3) by the Member States in the case of a dispute.

In Greece, the provision of e-signatures' certificates, either qualified or not, is regulated by Decision 248/71 of EETT[142]. EETT is recognised as the supervisory authority for the CSPs which are located in Greece (art. 9). art. 10 (2) states that "With the beginning of his activity, every CSP located in Greece shall notify in written form to EETT ... « information such as its name, address, phone number, legal status and services provided- for» the CSPs which issue qualified certificates to the public, apart from the notification a number of documents have to be submitted, namely: (a) statement of the CSP that he complies with the requirements set out in Annexes I and II of the MinisteriaI Decree and the Directive 1999/93, (b) Certification Practice Statement (CPS) of the CSP, which is a document that describes in detail the practice foIlowed by the CSP for the issuance of certificates and/or the provision of other certification services (art. 2), (c) documents proving the CSP's financial ability to cover any damage caused by its profession and (d) documents edited by the competent public or judiciary authorities proving that the CSP is not being under bancruptcy proceedings or mandatory management audit.[143]

The Decision contains some other important provisions, such as (a) that the CSP of qualified certificates is obliged to provide its customers with a 24 hour basis certification revocation service [art. 5 (5)], (b) that the same CSP must provide for a continuously updated directory of the valid and the revoked certificates [art. 5 (8)], (c) that the above CSP must maintain a 7-days-a-week revocation list service [art. 5 (9)], (d) that the same CSP must keep in written or electronic form a database including information (date of issuance, revocation, modification etc) about the qualified certificates it has issued [art. 7 (1)] and a database of all the qualified certificates it has issued for 30 years from the date of their expiration or revocation [art. 7 (2»), (e) that every CSP is obliged to notify EETT, its customers and all the other CSPs with which it has done business that he intends to stop operating at least three months before doing so [art. 6 (a)], (f) that the CSP which issues qualified certificates is obliged to inform its potential custorner at least for the latter's responsibilities flowing from the certficate' s use, for the code of conduct and the CPS of the *CSP* as well as for the conditions and the procedure of revocation (art. 8) and (g) that EETT has the right to check the compliance of the CSPs' functioning with the Ministerial Decree's provisions byinspections in the latters' place of business and imposition of the proper penalties (art. 12).

## Liability of CSPs

Considering the fact that CSPs act in a course of trade, faults on the provision of certification services may take place in various ways. Thus, for example, the CSP may not take proper evidence of its customer' s identity-either because of its negligence or due to misrepresentation on behalf of the customer-[144]; also, the CSP may not use security reliable technology, may not maintain a 24-hour-basis revocation list service or may employ dishonest or unskilled staff, reducing, as a consequence, its trustworthiness status.[145]

Liability issues could arise towards the CSP's customer-holder of a digital signature as could as towards the third party which transacts with the CSP' s customer and relies on the latter's identification as this is verified by the CSP's certificate. Directive 1999/93 acknowledges the above risks and provides for a minimum framework of liability rules. What has to be clarified is that the provisions of art. 6 of the Directive regulate the liability of CSPs issuing (or guaranteeing) a qualified certificate to the public and, thus, leave not only the functioning of CSPs in closed networks to be regulated by liability rules according to the contractual relationships between the members of those networks[146], but also the liability of CSPs that do not issue qualified certificates to be ruled wholly by national (contract) law.

Art. 6 refers to the liability of a CSP that issues a qualified certificate to the public "for damage caused to any entity or legal or natural person who reasonably relies on that certificate" [art. 6 (1)]. Thus, what is basically regulated by the Directive is the CSP' s liability towards the recipient of the electronically signed and certified message, namely the relying party. The CSP's liability towards its customer (the holder of the certificate) is, *prima facie,* left solely on the contractual relationship between CSP and customer[147]; however, it is suggested[148] that art. 6 could also be regarded as a minimum liability aspect that provides extra protection to the customer in addition to the contractual terms binding him. The notion of "reasonable reliance" of the third party on the qualified certificate is also crucial for the maintenance of trust between CSPs and the public. Apart from situations where the third party is technically expertised, it is logical to intrepret the reasonability or this party' s reliance with a minimalistic approach, i.e. to exclude CSP's liability only when the third party was extremely careless (did not check at all the compliance of the certificate with Annex I of the Directive).[149] On the other hand, the basis of liability for the CSP is negligence and not strict liability; the reason for that is that the CSP has the technical background to inspect in more depth any deficiencies related to its services and, thus, bears the burden of proovving that he did not act negligently when, for example, he collected the personal identification details of his customer.[150]

More specifically, art. 6 (1) refers to the obligation of a CSP to compensate the relying party ("entity, legal or natural person") for any damage caused as regards to: (a) the accuracy, at the time of issuance, of the information included in the qualified certificate and the existence of all the prerequisites prescribed (in Annex I) for a qualified certificate [art. 6 (1) (a)]

(b) the assurance that the identity of the holder of the certificate corresponds to the signatory of the electronic document whose signature is guaranteed by the certificate [art. 6 (1) (b)]

(c) the assurance that, in cases where the CSP produces both private and public keys, these products can be used in a complementary way [art. 6 (1) (c)].

In addition, art. 6 (2) makes the CSP liable if he negligently failed to register revocation of a qualified certificate. Furthermore, a CSP is allowed by art. 6 (3) to set a limit of liability according to the use of the qualified certificate-and, thus, not be liable for damage caused by further use- provided that this 1imitation is communicated to third parties. Additionally, the CSP is permitted by art. 6 (4) to set a limit on the value of the transactions for which the qualified certificate can be used-and, thus, be excluded from liability generating from damage caused after the exceeding of this limit-, given that this limitation is recognisable to third parties.

All the above provisions provide a minimum "advisory" but "binding" set of rules for each Member State's regulator when he intends to rule on CSPs' liability; this means that stricter rules may apply in order to enhance security, although extra care should be taken so as not to create barriers to entry in the CSPs' market by making the provision of such services financially inattractive and, as a result, eliminate competition. In Greece, the liability issue is not ruled by the Ministerial Decree 150/2001. Decision 248/71 does not contain any special provision; however, according to Annex I of the Decision, the Certification Practice Statement (CPS) of the CSP should contain, *inter alía,* an analysis of the responsibilities and the liability of the CSP towards its customers (para 3) and the relying third parties (para 8). The absence of such details gives EETT the right to impose appropriate penalties after inspection (probably to declare the functioning of the CSP invalid and stop its business), although no measure is being specified in the Decision.

## Cross-certiflcation within and outside the Community

Taking into consideration the universal nature of e-commerce operated through open networks like the Web, and also the need of the European Union for harmonised rules on certification services so as to achieve a competitive level on

that market, Directive 1999/93 provides for two aspects of e-signatures' services trade, i.e. intra and outside Community trade.

Art. 4 (1) mentions that "Member States may not restrict the provision of certification services originating in another Member State in the fields covered by this Directive". It also states that a CSP established in a Member State will be governed by the rules of that Member State. Thus, a CSP established, for instance, in Greece which provides certification services not only in Greece but also in France will be supervised and, if necessary, penalised by the Greek authority (namely EETT) and the French authority may not confine the CSP's activity. A problematic situation arises when the CSP is established in different Member States; which law will prevail is still a question that could be possibly dealt with if an intra-Community voluntary accreditation scheme-perhaps not quite demanding in relation to high technologies at the beginning- started operating so as to harmonise the different national laws applying in each case.Art. 4 (2) of the Directive provides for the free circulation of esignatures' products in the internal market provided that they cornply with the standards set out in the Directive. Thus, codes, private and public keys as well as advanced methods of e-signing (steganography, biometrics etc.) are free to flow through the Community with the intention to enhance security and promote ecommerce.[151]

With reference to the international aspects of providing certification services and selling e-signatures' products, art. 7 of the Directive intends to set up a friendly regime for CSPs established outside the Community. Thus, qualified certificates issued to the public by CSPs established in third countries must be recognised by national laws of the Member States as "legally equivalent" to those issued by intraComrnunity CSPs provided that: (i) the CSP established outside the Comrnunity complies with the provisions of the Directive and participates in a voluntary accreditation scherne of a Mernber State or, (ii) a CSP established in the Community guarantees the outsider CSP's certificate or, (iii) the outsider CSP's certificate is recognised under a bilateral or multilateral agreement between the Community and third countries. Three comments worth to be made here; firstly, that the Directive indirectly encourages the idea of CSPs being organised in voluntary accreditation schemes so as to facilitate the procedure of harmonisation of e-signatures' standards and the free transborder flow of e-products and services. Secondly, that by referring only to CSPs issuing qualified certificates, the Directive leaves the ruling of those CSPs issuing simple certificates to the national regulators, although the danger of discrimination and eradication of competition is perceptible. Thirdly, that in order to increase the level of competition and the investment in the European market, the Directive encourages the signing of bilateral or multilateral agreements between Member States and third countries. The same position is adopted by the Ministerial Decree ISO/2001 in its art. 5.

*PK1'B efficiency, key escrowing and key recovery*

Although public key encryption has been widely recognised as the most effective and financially suitable way of signing electronically, its compliance with increased levels of security has been doubted. Starting from the fact that a trusted third party is needed to guarantee extra security, because the pair of private and public keys is just a pair of numbers that does not guarantee the identity of its holder, the regulation of the activity of that party is regarded by many experts as troublesome and problematic. Moreover, even if the problem of identification is being solved by the provision of advanced certification services,[152] the CSP is not able to fully verify that the holder of the key pair was actually in possession of his private key during the disputed transaction, as factual circumstances like loss, threat or fraud are always likely to take place.[153] Deficiencies in the maintenance of revocation lists or false calculation of a private key's Iifetime are also some parameters which have to be taken into consideration by the CSPs when reassuring their customers for the quality of their services. And if we consider that Directive 1999/93 regulates in an appreciable extent only the issuance of qualified certificates, the question of how the 'simple' certificates are going to be treated arises automatically.

In addition, much debate has arisen on the issue of key esrcowing. Key escrowing is a system under which the holder of a private key deposits a copy of it with an escrow agent or, altematively, splits the key into several parts and deposits them with different agents (dispersion).[154] The idea behind that is that a superior authority wiIl be able to have access to the private key without having to gain that access directly from the holder. After having obtained a warrant by the courts, intelligence and law enforcement agencies will have access to any private key in order to fight terrorism or international crime.

Furthermore, key recovery is another similar alternative, based on the idea that the govemment or an organisation could set up a "key recovery centre"[155] where every interested key holder could send, through a message, a copy of his private key, so as, in cases of loss or dispute over it, the repository service could affirm its holder. However, it is being argued that by operating under a key escrow system, a private key is more vulnerable to on-line attackers as the security of the repository service can be harmed. In addition, it is suggested that the key holder loses the perfect control of his key as he further trusts its secrecy in another entity.[156] Key recovery has also been criticised not only on the fact that it violates the right to privacy and that it is an ineffective measure for the prevention of crime (criminals are likely to use "multilayered encryption"), but also on the costly infrastructure needed for its designation in a global level and on the danger of being attacked by information invaders.[157]

Directive 1999/93 states in Annex II (para j) that a CSP which issues qualified certificates must not "store or copy signature-creation data of the person to whom the certification-service-provider provided key management services". The same policy is followed by the Ministerial Decree (Annex II para j). It remains to the future to see if any dispute will arise over abuse of information stored in a govemmental repository; though, it is very likely that such interferences with citizens' private life will take place under the alibi of national security, prevention of crime or maintenance of public order.

## Conclusion-final remarks

Several aspects of the above analysis are crucial for the understanding of the e-signing's idea and function and, therefore, should be taken into account.

Firstly, it became plain that the geographical horizon within which the electronic signatures are operating is completely different from the "hand-shaking" scope where the.handwritten signatures work; the traditional bazaar has been substituted by the virtual marketplace and on-line commerce has no frontiers. Thus, electronic signatures apply Intenationally and their operation must be facilitated by the establishment of globally recognised technical standards which will ensure security on the Net.

Secondly, what was realised is that the existence of electronic signatures dependds, from a legal point of view, on the rules regulating the formation of contracts and their transforrnation in the Web world; the validity and admissibility of electronic contracts as evidence in legal proceedings go hand-by-hand with the legal recognition of e-signatures. Although paperless, the evolving on-line commercial practice still has as its cornerstone the notion of a contract which, in order to be binding for the parties, must be signed electronically in an impenetrable and bilaterally accepted way.

From a technical standpoint, the dissimilarity between the conventional methods of hand-signing and the modern techniques of e-signing is noticeable; from rubber stamps and seals we have moved to iris/handlvoice identification processes (biometrics) and elite technological solutions like steganography or quanturn cryptography. Public key encryption is the most widespread, easily performed, financially convenient and safe way of signing by electronic means, although many concerns on its efficiency in relation to faultless authentication and reliable certification have already arisen. Taking into consideration the tendency of Directive 1999/93 to encourage the one-sided development and "legalisation" of advanced electronic signatures, and bearing in mind the need for elevated criteria of trust which the market by itself imposes on its players, we can predict that in the ern-

ergent B2C and B2B as well as A2B and B2A markets novel forms of e-signing are likely to appear.

However, from a legal angle, handwritten and electronic signatures not only operate in the contract context but also serve the same purposes. In particular, they are used to identify the author of a document, to confirm his relationship with the written text and to reassure the reader that the signatory intented to be legally bound by the content of the scriptum; moreover, they guarantee for the integrity of the data content and prevent the signatory from repudiating in any sense (except if based on factual evidence) the validity of his signature. Electronic signatures additionally ensure the secrecy of the information exchanged via the electronic docurnent.

Therefore, manuscript and digital signatures should not be regarded as opponents but as contributors in the growth of e-commerce. By applying the idea of functional equivalence, the national legislators of the Mernber States shall try to harmonise the customary and the contemporary ways of signing by recognising to the latters the right to be treated as equal to the firsts and to be legally admissible in legal proceedings as evidence. Directive 1999/93 has taken the initiative, and the greek Ministerial Decree has followed; though, the categorisation of electronic signatures into "simple/non-qualified" and "advanced" blurs the field. It remains to the case law of each Member State to clarify the circumstances under which a "simple" e-signature can be faced as equal to an "advanced", elucidating in that sense the consumers when choosing the safest way of transacting on the Internet.

After having implemented the concept of electronic signatures, the European Commission has moved cautiously to the next stage, namely the establishrnent of an open rnarket for e-signatures' products and services. By not recognising any e-signing practice as the ultimate method, Directive 1999/93 approaches cryptography and other techniques with a technologically neutral manner so as to hearten the entrance of new players into the market, reinforce competition within and outside the Community and build a safe environment for on-line commerce. Products other than codes and keys are quite likely to come into view in the e-commerce panorama. In the services' area, by putting into operation the practice of voluntary accreditation of Certification Service Providers (CSPs), Directive 1999/93 has moved one step further; the participation of CSPs in such schemes where the compliance with high-tech standards is compulsory, not only toughens competition and promotes technology through research and innovation but also, and more significantly, builds up a 'firewall' of security on the Web. Recently, the European Commission has demonstrated its agony for the establishment of a safer digital signature marketplace and the opening of the european

market to third countries with its Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions "Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market" [COM(2008) 798][158].

Furthermore, for the effective function of public key encryption, the existence of a Trusted Third Party is necessary. The connection between the actual identity of the signatory with his public key is of fundamental importance and the CSPs provide an alternative for the "physical presence" model which applies in the traditional trade.

Not surprisingly, the vital role which the CSPs play is accompanied by a number of legal issues. For instance, Directive 1999/93 (and the Greek Ministerial Decree 150/2001) states that only the "qualified" certificates a CSP issues can give automatically legal validity to an electronic signature. In addition, the designation, supervision, liability and cross-certification of CSPs issuing 'simple' certificates is left to the discretionary power of the national legislator, while for the CSPs that provide qualified certificates the same issues are dealt with in accordance to a minimum legal framework provided by the Directive itself. This "two-tier" approach, though inevitable for this embryonic phase of the e-signatures' market where the priority seems to be the involvement of as many CSPs as possible, is probable to cause uncertainty in the consumers' and businesses' field. Voluntary accreditation schemes in national as well as in European level would be a way out; in a more mature stage of the market, a slight moving away from the technological neutrality principle by replacing voluntary with mandatory accreditation could give a better solution, provided that foreclosure of the relevant markets is avoided.

Focusing on CSPs that issue qualified certificates to the public, their designation, functioning, supervision, liability and cross-certification throughout the Community is regulated by national laws that have to comply with the provisions of Directive 1999/93. Thus, for instance EETT is the Greek authority which sets out the insitutional precondition for the designation of a CSP, the technical standards which have to be followed, the ways and consequences of the supervision as well as the liability rules applying to each case and the cross-certification modus operandi. It is obvious that the better a national law adopts the Directive's provisions (from matters such as the compliance of the CSPs; technology with European and international standards to issues such as the ensurance of the reliability and state-of-the-art knowledge of the CSPs' staff), the more stable the structure of e-commerce becomes.

From a consumer protection viewpoint, the on-line customer not only is not deprived of the protection of national and international legislation on consumer protection, but also is placed in an advantageous position when dealing with a negligent CSP's mediation; the latter (CSP) has the burden of proving that it did not act negligently during the provision of certification services like time-stamping, public key registration and directory or revocation listing. The net-ignorance of the consumer is compensated by firm obligations imposed on the CSPs.

Moreover, from a data protection position, it became clear that the provision of key escrow and key recovery services has to be scrutinized before implemented; the dangers it encloses for the privacy and the self-determination of the individual in the information society should be fairly balanced with the actual need for maintenance of public safety and national security.

Finally, it was comprehended that the motivation of any legislative attempt on electronic signatures does not rely solely on the grounds of technical applications but is rather a subsequence of public measures; thus, the European Union, by adopting Directive 1999/93, apart from harmonised standardisation and financial integration, has aimed at fortifying the e-commerce practice in the Community and toughening the levels of competition with the US market. In a microscopic level, similar should be the purpose of the Greek legislator in relation to the presence and the potential leading position of Greece in the Balkan territory's on-line commercial regime.

In a nutshell, behind the idea of electronic signatures there is the need for trust in an electronic environment characterised by anonymity and unlimited manipulation. The challenges which the traditional rules on forgery or fraud face are multiple as advanced technology becomes a dangerous weapon in the hands of competent but malicious netizens. While establishing a primary field of e-signing, policy-makers should place great emphasis on Intemet security.The future will show if "a technology born of distrust can become a guarantor of trust in the online world".[159]

## Endnotes

1. Ian J. Lloyd, "Information Technology Law" 3fd edition, Butterworths 2000, p. p. .29-31.
2. See also recital14 of Directive 1999/93 on Electronic Signatures.
3. Treaty establishing the European Community (consolidated text) OJ C *325,24/1212002,* art. 3 (1) (c), 23 and 24, http://europa.eu.intleur-lex/enlsearch/searchtreaties.html, visited 24/08/2003.
4. Their use is also apparent in the public administration system, in goveГnmentaI organisations, in intelligent agencies (where the further issue of key-escrowing arises) etc.
5. European Commission, "Communication to the Eui-opean ParJiament, the Council, the Economic and Social Committee and the Committee of the Regions: A European Initiative in EJectronic Commerce", COM (97) 157, Brussels, 15/04/97, p. 2.
6. Ibid. p. 2.
7. Arno R. Lodder and Henrik W.K Kaspersen, "eDirectives: Guide to European Union Law on ECommerce-Commentary on the Directives on Distance SelJing, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection", Kluwer Law International 2001, p. 3.
8. Ronald de Bruin, "Consumer Trust in Electronic Commerce: Time for Best Practice", Kluwer Law International 2002, p. 6.
9. Directive *9717fEC* on the protection of consumers in respect of distance contracts, OI L 144/19, 4.6.1997.
10. Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000.
11. Arno R. Lodder and Henrik W.K. Kasparen, id., p. 3
12. Lilian Edwards and Charlotte Waelde, "Law & the Internet: a framework for electronic commerce", Hart Publishing 2000, p. 18.
13. Ibid p. 20.
14. See Eloin Philipopoulou, «The legal framework of electronic commerce», Dikaio Epjheirjseon aki Etairion (Year 6) (in Greek), p. 1087.
15. Ibid p. 22.
16. Ibid p. 22, where the postal rule is referred as an exemption to the general rule that a contract is concluded once the acceptance is sent and received by the offeror as it sets out that if the acceptance is sent by post (and not, for instance, by telephone or telefax), it becomes effective ''once posted, rather than when it is received".
17. Ibid p. 25.
18. Ibid p. 25, where a click wrap contracting procedure is considered as different to e-mail contracting in two ways, namely because during the first the communication between offeror and offeree is instantaneous and also because the practice of traditional negotiation of the terms of the contract that can take place through e-mails is replaced by the ''I accept" or ''Yes" technique that applies to click wrap agreements.
19. Ibid p. 29; EC Directive on E-commerce art. 1O (1).

20. Ibid p. 31; EC Directive on E-commerce art. 1O (1),(2).
21. As set out in the Rome Convention on the Law Applicable to ContractuaI Obligations *(8OI934IEEC),* OJ L 266, *09/10/1980,* art. 3.
22. Rome Convention, art. 5 (1); EC Directive on E-commerce, art. 2 (e).
23. Ibid art. 5 (2).
24. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *OJ* L 13/12,19.1.2000, art. 5 (1).
25. International Covenant on Civil and Political Rights art. l7, which declares that "no one shall be subjected to arbitrary or unlawful interference with his privacy ... ";general comment 16 states" The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by Jaw», http://www.unhchr.ch/html/menu3/b/accpr.htm. visited 25/08/2003.
26. European Convention on Human Rights art. 8 (respect for private life with the exemption of interference permitted due to, *inter alia,* national security and public safety reasons) http://www.echΓ.coe.jnUEng/BasicTexts.htm, visited *25/08/2003;* Directive *2002158/EC* on privacy and electronic communications OJ L 201/37,31.7.2002.
27. Greek Law No 2472/1997 on the protection of individuaJs with Γegard in the processing of personal data http://www.dpa.gr/DocumentsIEng2472engll.doc. visited *25/08/2003.*
28. United Nations Commission on InternationaJ Trade Law (UNCITRAL) Model Law on Electronic Signatures 2001 http://www.llncitral.org/engJish/texts/eIectcom/inl-elecsi_g-e.pdf, visited *26/08/2003.*
29. American Bar Association Digital Signature Guidelines 1996, http://w\VW .abanet.org/scitech/ ec/i sc/ ds g -tutorial.htmI, visited 26/08/2003.
30. Rosa-Julia Barcelo, "The German Legal Situation after the 'Digital Signature Law'", *http://www.droit.fundp. ac.be/textes/addendum.* pdf, visited *26/08/2003.*
31. FEK Issue *125/*A/25-6-200l, *http://www.gspa.gI-ıINETDHES/diadp/b-2-1-S.htm.* (in Greek), visited *26/0812003.*
32. Konstantinos N. Christodoulou, «Electronic Documents and Electronic Contract» (in Greek), Ant. N. Sakkoulas 2001, p. 174, where the author supports the view that, for reasons of technologicaI neutrality and improvement of e-commerce policy, the European Union has plIrposively left the field of electronic signatures that can be admitted as valid open to adjustments according to technology r:rogress.
33. Although the location of the signature should not be a precondition of its vaJidity except if such a requirement is imposed by law,as it happens in the wilIs where each page must be signed by the testator and the witnesses,Adrian McCullagh, "Signature Stripping: A Digital Dilemma», *http://eJi.warwick.ac.ukliiltJO* l-l/mccullagh.htmJ, visited *27/05/2003,* p. 4.
34. Chris Reed, "What is a Signature?", *http://eIi.warwick.ac.UKJiltOO-3/reed.html,* visited *27/05/2003,* p. 1.
35. Karmini Bharvada, "Electronic Signatures, Biometrics and KI in the UK", Internationa\ Review of Law, Computers & Technology, volume 16, N. 3, 2002, p. 266.
36. Endnote [34], p. 2.
37. Endnote [35], p. 267.

38. Ibid p. 267.
39. Endnote [32], p. B.
40. Nicholas Bohm, Ian Brown & Brian Gladman, 'EIectronic Commerce: Who Carrries the Risk of Fraud?", http://eli.warwick.ac.uk/iiJtlOO-3/bohm.htmJ, visjted 28/05/2003, p. 8.
41. Endnote [7], p. 42, where it is held that this would be admitted as e-signing only if based on arl.5 (2) of Directive 1999/93.
42. Endnote [35], p. 269.
43. Ibid p. 270.
44. Ibid p. 270; also, Nigel Hawkes, «Machines wiIl pay up in blink of an eye», http://www.cl.cam.ac.uk/users/igdl000/atm.ipg. visited 27/08/2003; aIso,http://members.fortunecity.comlpawanjanbandhu/biometric_signatures.htmI, visited 27/08/2003, where it is held that, aIthough advanced, the iris technique has a sIight possibility of mistake every time due to factors such as "reflections from eyeglasses, motion blur, noise in the camera etc".
45. Endnote (35], p. 270.
46. Endnote [34], p. I3; also, http://WWw,Dscom.co.uk./products/signature/, visited *27/0812003,* where it is said that pressure, rhythm, ink flow, timing and speed are the criteria of the examination of the authenticity of a digitised pad' s signature.
47. Endnote [35], p. 271.
48. Ibid p. 271.
49. Declan McCullagh, «Bín Laden: Steganography Master?», httP://www.wired.com/news/PωJıtıcs/O.I283.41658.00.html. visited 27/08/2003.
50. Endnote [33], p. 272.
51. http://www.cs.dartmouth.edul-/ford/crypto.html. visited *27/08/2003.*
52. Sarah Andrews, "Who Holds the Key?-A Comparative Study of US and European Encryption Policies", http://eli.warwick.ac.ukJiltlOO-2/andrews.html, visited *27/05/2009,* p. 2.
53. Endnote [8], p. 52.
54. Lorna BrazeIl, 'EIectronic Security:Encryption in the Real World", EIPR 1999,21 (1), pp. 18-19.
55. Endnote [8], p. 51.
56. Mukul Pareek, "Cryptography-a primer", http://www.financeoutJokk.comlcryptography.htm. visited 27/08/2003, where the 'computationaJ infeasibiJity' concept is regarded as a standard for KI encryption because:» 128-bit encryption has never been broken ... it wouId take a years to crack 128-bit encryption using today's technoJogy".
57. John Angel, «Why Use Digital Signatures for Electronic Commerce?», http://eIi.warwick.ac.uk/iilt/99-2/angeI.html, visited 27/05/2009, *p. 4.*
58. Steffen Hindelang, "No Remedy for Disappointed Trust- The LiabiJity Regime for Certification Authorities Towards Third Parties Outwith the EC Directive in EngJand and Germany Compared", httP://elj.warwick.ac.uk/iiItJ02-IIhindelanp:.html, visited 27/05/2003, p. 4.
59. Endnote [56], «a key, which is a user selected password, number OY 'passphrase', is used as a rıarameter in the encryption algorithm to convert the plaintext to encrypted text".

60. Endnote [8], p. 51 (footnote 70): «The digital signature itself consists of a signed message digest that often is attached to the message itself. Typically, the digital signature is sent along with the message to the receiver».
61. Endnote [8], p. 51 (footnote 70): "The hash function has the property that, if the message is changed in any way, even by just one bit, an entirely different value will be produced by the hash function".
62. The influence of UNCITRAL Model Law on Electronic Signatures, http://www.uncitral.org/en-index.htm, visited 25/05/2010, is obvious, as in art. 2 (a) electronic signature is defined as "data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message".
63. See also Preamble of UNCITRAL Model Law, para 8.
64. Crhistina Spyrelli, "Electronic Signatures: A Transantlantic Bridge? An EU and US Approach Towards Electronic Authentication", http://www.elj.warwick.ac.uk/jilt/02-2/spyrelli.html, visited 27/04/2009, p. 4.
65. From a Greek point of view, this distinction is interpreted as if the "simple e-signature" can be used in any transaction where no formality is needed while the "advanced" e-signature can be used in all the other transactions that require formalities as equivalent to handwritten signatures, see John D. Iglezakis, "The legal provisions on Digital Signatures Directive 1999/93 and National Laws", Episkopisi Emporikou Dikaiou C/2000 (in Greek), p. 633.
66. An indirect reference is being made in art. 1721 para 1 of the Civil Code that refers to the handwritten last will, where, apart from being written by the testator's hand itself, it must be written by his hand in whole, see Chryssoula Michaelidou, "The electronic signature's problem", Dike International 31 (2000) (in Greek), p. 1203.
67. Although in commercial transactions no formality is being required in Greek practice, see N.K.Rokas, "Modern Technology and Commercial Law", Episkopisi Emporikou Dikaou 1998 (in Greek), p. 7. See also Anastasia Papathoma-Betge,"Electronic commerce: Legal issues on the transactions on the Internet", Dikaio Epihiriseon kai Etairion (year 5, in Greek), p. 1240.
68. D. Maniotis, "The digital signature as a means of confirming the validity of documents in civil procedure" (in Greek), Ant.N.Sakkoulas publishing 1998, p. 35.
69. Still, case law has broadened the horizon of handwrtiting by recognising as legal valid signatures put by foot or mouth or signatures created by technical means such as fax or telex.
70. Endnote [68], pp. 83-87.
71. Definitions of "signature-creation data" and "signature-verification data" respectively.
72. After being penalised, for example, by the European Commission, the European Court of First Instance or the European Court of Justice for not having implemented in a satisfactory degree the Directive's provision on data protection, consumer protection or Certification Authoritie's (CA's) designation etc.
73. This is also obvious by art. 1 para. 1 of the Directive, where the dual purpose of the Directive is "to facilitate the use of electronic signatures", and not to exhaustively rule it, and "to establish a legal framework fro electronic signatures and certain certification services in order to ensure the proper functioning of the internal market", and not to regulate in detail on their legal recognition. See also Endnote [7], p. 40. See also recital 4 of the Directive, where

the framework provided by the Directive intends to "...strengthen confidence in, and general acceptance of, the new technologies".

74. As noted down in Annexes I, II, III, IV.
75. See Vassilis Karagiannis, "The legal protection of electronic data exchange", Dikaio Epihiriseon kai Etairion (year 6, in greek), p. 29.
76. Endnote [57], p. 3.
77. Endnote [64], p. 2.
78. See also recital 8.
79. Jamie Murray, "Public Key Infrastructure, Digital Signatures and Systematic Risk", http://eli.warwick.ac.uk/Jilt03-lImurray.html, visited *29/07/2009,* p. 3.
80. As weII as for, e.g., the reader of a last wiII on which some parts of the text have been scratched, rewritten or deleted without having been signed, although there is a slight difference: any alterations on an electronic message are hardly detectable, while forgery on manuscripts is demonstrable with the help of graphology (see, e.g., http://www.apogeegraphology.com/lectures.html. visited 28/08/2009).
81. Endnote [8], p. 51 (footnote 70).
82. Chapter 1 (B) (b).
83. Art. 2 (4).
84. Art. 2 (5).
85. Art. 2 (6) in combination with Annex ΠΙ, where the need for extra security appears through the use of phrases such as «the signature-creation-data used for signature generation can practicaIly occur only once" (para 1) (one-way function), "secrecy reasonabJy assured" (para 1), "the signature creation data ... be reliably protected by the legitimate signatory against the use of others" (para 2) etc.
86. Art. 2 (7).
87. Art. 2 (8).
88. Art. 2 (12).
89. Stewart A. Baker & Paul R. Hurst, "The Limits of Trust Cryptography, Governments and Electronic Commerce", Kluwer Law International 1998, p. 4.
90. Endnote [8], p. 13.
91. Kevin Scott Boomsma, "The Key Escrow Debate", http://raphaeI.math.uic.eduJ#ieremy/crypt/contrib/boomsma2.htmI, visited 29/08/2003.
92. See aIso recitaI 18 "The storage and copying of signature-creation data could cause a threat to the legaI validity of electronic signatures".
93. Stephen Mason, "The Evidential Issues Relating to Electronic Signatures-Part 1", Computer Law & Security Report Vol. 18 no.3, 2002, p. 175.
94. Non-repudiation can be divided into «non-repudiation of origin» which prevents the creator of the message from claiming that he did not send it, and «non-repudiation of delivery» which prevents the message's recepient from denying having received it, endnote [8], p. 14.
95. James M. Galvin, «Authentication, Non-Repudiation and Secure Electronic Signatures», http://lists.commerce.net/archives/ts-portfoiio/199709/msgOOOOl.html, visited 29/08/2009.

96. Art. l para 2.

97. Art. 5 (l) (b).

98. See also recital 21:" ... this Directive ... does not affect national rules regarding the unfettered judicial consideration of evidence".

99. Which, in closed networks where "contractual relationships and mutual trust already exist" between the users *(http://www.freenix.fr/netizen/chiffre/ecryptol.html*. visited *29/08/2009),* is not as doubted as in semi-open networks like "the internal networks of companies" *(http://www.ficora.fi/englantiltietoturva/suoiausm.htm*. visited *29/08/2009)* or in open networks like the Internet.

100. The "structural integrity" of a record, i.e. the non-alteration of its structure ( structure="jts physical and logical format and the relationships between the data elements comprising the record"), is a special aspect of integrity, *http://www.archives.gov/records* management lpolicy and guidance/signature technology. html, visited *29108/2003*.

101. The use of "secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify or delete electronic records» (http://www.temple.edulphal'macv QARN8, visited *29/08/2009)* is also encouraged by Directive *1999/93* which, in recital 9 refers to "time-stamping services" or "computing services".

102. Adrian McCullagh & William Caelli, "Non-Repudiation in the DigitaI Environment», *http://www.tirstmonday.dk/issues/issue5* 8/mccullaghl, visited *29108/2003*.

103. Endnote [57], p. 5.

104. Endnote [34], p. 9.

105. Vincenzo Sinisi, Sinisi Ceschini Mancini & Partners, Rome, «Digital Signature Legislation in Europe», Butterworths Journal of International Banking and Financial Law, January 200 I, p. I7.

106. and the mathematical procedure that follows the application of that private key to the encryption algorithm.

107. Considering that a signature can be stored in a computer's hard disc, a floppy disc, a removable disc or a smart card (for smart cards see, e.g. http://www.\.Iayrnaker.se/bitonline/2003/05/23/20030523BIT0031O/0523003I.htm, visited 30/08/2003), it can be realised how easily a private key could be attacked, lost, stolen or destroyed and, as a result, the risk of forgery and fraud the owner of that key runs. http://www.ac. uk. pgp. netlpgpnetlsecemaillq4/node8.html. last visited 30/8/2009.

108. Endnote [57J, p. 6, where the author says: «Instead of creating a cornplete new Iegal framework, existing achievements shouId be advised, as far as they are compatible with it».

109. Provided that it is an advanced signature based on a qualified certificate and created by a secure signature-creation device [art. 5 (1)].

110. Perhaps because the other forms of e-signing (biometrics, steganography, quantum cryptography etc) apart from KI encryption have not developed enough so as to create the need for special and separated legislative treatment.

111. http:///www.irc.cec.eu.int/download/press/newsletters/letter200005-en.pdf,visited30/08/2009, p. Z 1]2 Decision 1327/2001 of the One-Member Magistrate Court of Athens.

112. http://www .dsanet. ψ: 83 80/W ebtop/ws/alis9i/www/case/Record?set=6&m= 17 &sid=26, visited *30/08/2009* (in Greek).

113. It is common knowledge that a person can have more than one e-mail addresses, even by having provided false personal information to the ISP. ''Eavesdropping" is another technique for diverting emails from the real owner and forging his e-signature, http:// www.ac. uk. pgp. netlpgpnetlsecemaillq4/node8.html. visi ted 30/08/2001.

114. See Konstantinos N. Christodoulou, «Order for payment based on electronic document» (in Greek), Dike International 32 (2001), pp. 457-471.

115. This is permitted by art. 6 (4) of the Directive; see also, e.g., http://www.adacom.gr/ engIish/frames.htm. visited 30/08/2009.

116. Christopher Reed, "Internet Law: Texts and Materials", Butterworths, 2000, p. 119 (The phrase originates from a cartoon, http://www.cartoonbank.com/product details.asp ?mscssid=DA 1 DH4 UJDG459HA VC4PMEVB218TG 24TB&sitetype=1&did, visited 30/08/2009).

117. Endnote [79], p. 3.

118. in contrast with biometrics, where the use of fingerprints or iris colour verify in an unmistakable way the identity of the person acting as advanced electronic IDs.

119. Caroline Copeland, "DigitaI Signatures: Throw away your pens", Entertainment Law Review2000, 11 (5), p. 112.

120. Endnote [57], p. 4; in Greek law, this problem would be dealt with by PenaI law (fraudulent use of signature) and Civil law (damage on the right of the person on his name).

121. In contrast with closed networks where the levels of trust are highly based on personal relationships and voluntary agreements., see recital 16 of the Directive.

122. Stephen Mason, "The Evidential Issues Relating to Electronic Signatures-Part II", Computer Law & Security Report Vol. l8 no 4 2002, p. 244.

129. Namely: www.eurobank.gr, www.adacom.com, www.edps.gr, www.ase.gr/repository, www.ypesdda.gov.gr, www.geniki.gr, www.eap. gr, www.ktpae.gr and www.acci. gr,visited 30/05/2010.

130. http://www.acci.gr/enindex2.htm. visited 30/05/2009.

131. Ar1.2 (10): "Qualified certificate means a certificate which meets the requirements laid down in Annex I and is provided by a certfication-service-provider who fulfills the requirements laid down in Annex Π».

132. OJ L 289, 16/11/2000 p. 42.

133. http://www.eett.gr/engpages/index2.htm. visited 27/05/2003 . See also Decision 248/71 (FEK Issue 603/B/16-05-2002), http://www.eett.gr/opencms/export/sites, visited 25/05/2010, Regulation on the Provision of Electronic Signature Certification Services (FEK Issue 284/A/22-11-2002), Regulation 295/63 on the designation of bodies for the conformity assessment of secure-signature-creation devices and secure cruptographic modules and on the designation of bodies for the conformity assessment of certification service providers using the voluntary accreditation criteria, http:www.eett.gr/opencms/ export/sites/deefault/EETT_EN?Electronic-Communications/DigitalSignatures/295-63.pdf, visited 25/05/2010, Regulation 295/64 on the conformity assessment of secure

signature creation devices and secure cryptographic modules, Regulation 295/65 on the Voluntary accreditation of the certification service providers.

134. Art. 2 (11).

135. Endnote (119], p. 28.

136. Prior authorisation is defined in recital 10 as " ... not only any permission whereby the certificaltion service provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect".

137. Endnote [7], p. 48.

138. The market forces' concept drives the stucture of the e-signatures' market; see, e.g., "Questions and Answers from EEMA's European Electronic Signatures Directive Workshop, November 2001, Brussels, http://www.eema.org/SProiects/esigqa.asp, visited *01/09/2009*, "The value of a qualified eIectronic signature depends on market demand".

139. http://www.tscheme.org, visited 01/09/2003; see also, http://www.ecp. nl, visited 02/09/2009.

140. see http://www.eett.gr/engpages/index2.htm. visited 27/05/2009.

141. Endnote [7], p. 51; see, e.g., http:I/www.europa.eu.ıntlıformatíonsocıety/eeurope/actionplan/safe/esignaturesindex_en.htm, visited *02/0912009*, where we read that Germany, Austria and Denmark provide for mandatory notification, while in the Netherlands CSPs issuing qualified certificates have to register to OPTA which "does not conduct an assessment before registration" *(http://ww* w. opta. nl/index.asp? /url=recentinformatio *nl* document.asp&id= 1 063&thema id=O&prevurl= %2Findex&2Easp, visited 02/09/2003).

142. Decision on the provision of electronic signatures' certification services (FEK Issue 603/BIl6-052002).

143. See Konstantinos N. Christodoulou, «Three new issues on the electronic signatures' law after the Greek draft on electronic signatures", Dike International 31 (2000), p. 1033.

144. Michael Froomkin, 'The Essential Role of Trusted Third Parties in Electronic Commerce", http://www/law/miami.edu/-froomkinlarticles/trustedl.htm. visited *02/09/2009*.

145. Endnote [57}, p. 6.

146. RecitaI 16; see a1so, Endtnote [7J, p. 58.

147. And probably to the consumer protection Iaw applying to each contractuaI relationship 148 footnote [7], p. 59.

149. Ibid p. 60.

150. Ibid p. 61; Directive art. 6 (1) (c).

151. See Nancy Muenchinger and Adam Mekaoui, "Regulatory Aspects ofElectronic Signatures", Computer Law & Security Report Vol. 18, vol. 2002, 29.

152. Though the possibility of misrepresentation of the holder is high, as the classification of certificates system does not require strong identity proof for all the categories when registering.

153. Carl Ellison & Bruce Schneier, "Ten Risks of PKI: What You are not Being Told about public Key Infrastructure», Computer Security Journal Vol. xVI, Number 1, 2000, p. 6.

154. Endnote [54], p. 20.

155. Ibid p. 21.

156. Ibid p. 20.

157. Endnote [52], pp. 4-5.

158. http:www.europa.eu./legislation_summaries/information_society/l24118_en.htm,25/5/2010.

159. Endnote [89], p. 5.

## Bibliography

### *Books*

Arno R. Lodder and Henrik W. Kaspersen, «eDirectives: Guide to European Union Law on E-Commerce", Kluwer Law Intenational 2002

Christopher Reed, ''Intemet Law: Texts and Materials", Butterworths 2000 D. Maniotis, "The digital signature as a means of confirming the validity of documents in CiviI Procedure" (in Greek), Ant.N.Sakkoulas 1998

Ian J.Lloyd, "Information Technology Law", Butterworths 2000, 3rd edition

Konstantinos N. Christodoulou, 'EIectronic Documents and Electronic Contract» (in Greek), Ant.N.Sakkoulas 2001

Li1ian Edwards & Charlotte Waelde, "Law & the Intemet: a framewor for electronic commerce", Hart Publishing 2000

Roland de Bruin, "Consumer Trust in Electronic Commerce: Time for Best Practice", Kluwer Law Intenational 2002

Stewart A. Baker and Paul R. Hurst, «The Limits of Trust: Cryptography, Govemments and Electronic Commerce», Kluwer Law International 1998

### *Articles*

Adian Mc Cullagh, William Caelli and Peter Little, "Signature Stripping: A Digital Dilemma», *http://elj.warwick.ac.ukljiltlOl-1/mccullagh.html*, visited *27/05/2003*

Anastasia Papathoma-Betge, 'EIectronic commerce: Legal issues on the transactions on the Intemet" (in Greek), Dikaio Epiheiviseon kai Etairion (Year 5), p. 1237

Carl ElIison and Bruce Schneier, "Ten Risks of PKI: What You are not Being Told about Public Key Infrastructure", Computer Security Joumal Vol. XVI, Number 1, 2000

Chris Reed, "What is a Signature?", *http://elj.warwick.ac.ukliilt/OO-3/reed.html*, visited 27/05/2003

Chryssoula Michaelidou, "The electronic signature's problem" (in Greek), Dike Intenational 31 (2000) p. 1188

Christina Spyrelli, «Electronic Signatures: A Transantlantic Bridge? An Eu and US LegaI Approach Towards Electronic Authentication», http://eli/warwick.ac.uk/iilt/022/Spyrelli.htmI, visited *27/05/2009*

Caroline Copeland, "Digital Signatures: Throw Away Your Pens", EntLRev 2000, 11 (5)

Elli Philipopoulou, «The legal framework of electronic commerce», Dikaio Epiheiriseon kai Etairion (Year 6) p. 1086

Ioannis D. Igglesakis, «The legal provisions on digital signatures: Directive 1999/93 and national laws" (in Greek), Episkopisi Emporikou Dikaiou *Cl2000,* p. 619

Jamie Munay, «Public Key Infrastructure, Digital Signatures and Systematic Risk», http://eli.warwick.ac.ukliilt/03-1/murray.html, visited 29/07/2009

James Backhouse, ''Assessing Certification Authorities: Guarding the Guardians of Secure E-commerce?", Journal of Financial Crime Vol. 9 No 3, 2002, pp. 217-226

Jeremy Newton, "The European Directive on Electronic Signatures", EBL, March 2002, p. 5

John Angel, «Why use Digital Signatures for Electronic Commerce?», http://eli.warwick.ac.uk/iilt/99-2/angel.html, visited 27/05/2003

Kamini Bharvada,"EIectronic Signatures, Biometrics and PKI in the UK", International Review of Law, Computers & Technology Vol. 16, No 3, pp. 265-275, 2002

Konstantinos N. Christodoulou, ''Order of payment based on electronic document" (in Greek), Dike International 32(2001), p. 457

Konstantinos N. Christodoulou, «Three new issues on the law of electronic documents after the bill on electronic signatures" (in Greek), Dike International 31(2000), p. 1006

Lorna Brazell, "Electroníc Security: Encryption ín the Real World", EIPR 1999, 21 (1), 17-27

Nancy Muenchinger and Adam Mekaoui, "Regulation Aspects of Electronic Signatures", Computer Law & Security Report Vol. l8, 2002

Nikos K. Rokas, «Modern Technology and Commercial Law» (ín Greek), Epiotheorisi Emporikou Dikaiou 98

Richard Hamson, «Public Key Infrastructure: The Risks of Being Trusted», C&L, August/September 2000

Sarah Andrews, «Who HoJds the Key?-A Comparative Study of US and European Encryption Policies", *http://eli.warwick.ac.ukliilt/00-2/andrews.htrnl*, visited *27/05/2003*

Steffen Hindelang, "No Remedy for Disappointed Trust-The LiabiIity Regime for Certification Authorities Towards Third Parties Outwith the EC Directive in England and Germany Compared", *http:lleliIwarwick.ac.uklíilt/02-1/híndeIang.html*, visited 27/05/2009

Stephen Mason, «The Evidential Issues Relating to Electronic Signatures-Part Γ, Amicus Curiae Issue 45 January February 2003

Vassilis S. Karagiannis, "The legal protection of electronic data exchange", Dikaio Epiheiriseon kai Etairion (in Greek) (Year 6), p. 19

Vincenzo Sinisi, Sinisi Ceschini Mancini & Partners, Rome, "Digital Signature Legislation in Europe", Butterworths Joumal of IntemationaI Banking and Financial Law, January 2001

# Ethics, codes of conduct and p2p

Irini A. Stamatoudi

## Introduction

Ethics is not a term which is particularly linked to copyright. The reason for this is that ethics usually apply to those areas of law which are either obscure or under formation (like for example, cultural property law). In these areas the interests of the parties (which are strong) are directly opposite and therefore solutions can only be reached on the basis of the parties' goodwill and consensual practices. We can hardly argue that copyright law is under formation; not because the interests involved are not strong and in cases directly opposite, but because those interests have in most cases been reconciled by the existing law in the area. Yet, there are areas in copyright law which are obscure. That means that a definite solution to a matter is not expressly provided in the law by reason of the fact that such solution has not ripen yet so as to be adopted, or because there is the conviction that self-regulation can be more effective and less intrusive, or simply because the political will is not there to provide for such solution. A characteristic example in this respect is copyright protection and the file exchanging systems on the Internet known as peer-to-peer (P2P).

This issue is highly interesting in copyright law for various reasons. Just to name a few, P2P is a practice, which is relatively new and inextricably linked to technological developments. That means that file sharing during recent years has known different forms and shapes essentially depending on the software used. In addition to it, P2P is a tremendously popular practice in the sense that it is easy and cheap to share files of protected material on the Internet and in most cases the quality of the shared content is comparable, if not the same, with the original work. On top of it, it involves a considerably high number of people having access to the Internet irrespective of age, profession, and so on, and knows no territorial boundaries. On top of everything, it also has to do with immaterial property (i.e. copyright) which is traditionally faced with difficulties with regard to sensitizing people as to its significance as a property right.

It is clear, of course, that P2P practices involve Internet Service Providers (ISPs).

ISPs are the intermediaries which technically provide the means to access the Internet,[1] through the assignment of IP addresses. In fact, the connection and communication of private computers on the Internet is based on IP addresses. IP ad-

dresses are numerical address formats, comparable to a telephone number, which enable networked devices, such as webservers, e-mail servers or private computers, to communicate with one another on the Internet. IP addresses can either be static or dynamic. Static IP addresses are assigned in order to connect private users to the Internet in the same way they are connected to a telephone network. However, this is not always the case, since the Internet is at present still organised in such a way that each access provider has only a limited number of addresses available to it. For this reason subscribers are assigned dynamic addresses. Dynamic IP addresses are assigned to subscribers on an *ad hoc* basis from the limited number of addresses the ISP has. Thus, these addresses change each time a subscriber dials up.[2]

On the part of copyright law, it is clear that the exchange of files on the Internet does not fall within an exception to the exclusive and absolute rights of authors and rightholders of related rights. Even if it is argued that file sharing may come under the private copy exception, it would however fail under the three step test in the sense that it would conflict with the normal exploitation of a work and would unreasonably prejudice the legitimate interests of the rightholders.[3] That translates into the fact that when one downloads songs or films from the Internet, this very person, will not buy them on the market to watch or to listen to them since his needs have already been covered. That means that this practice conflicts with the normal exploitation of the work and unreasonably prejudices the legitimate interests of the rightholder.

It should be noted at this point that ethics in this area take more the form of good practices and ethical conduct (set of rules outlining the responsibilities of or proper practices for an ISP)[4] rather than ethics *stricto sensu*[5] or, even more precisely, applied ethics that provide how moral outcomes can be achieved in specific situations. If we are now to see the relation between ethics, codes of conduct and copyright protection, we could schematically argue that ethics form the principle, codes form the vehicle and copyright protection forms the ultimate target.

The aim of this paper is to a) discuss the emergence of codes of conduct in the area of copyright law and in particular in P2P, b) discuss some examples of such codes, and c) examine whether self-regulation and the voluntary adoption of codes of conduct can form and transform ethics and provide a viable alternative to law.

## The Role of Codes of Conduct

### *Provision in Law*

Self-regulation, as well as voluntary codes of conduct, are concepts whose sperms are found in antiquity. One example is the Hippocratic oath taken by doctors. However, a proliferation of such codes in different sectors has coincided with

increased emphasis on particular problems in the sector itself. For example, the 1990s saw a proliferation of corporate codes of conduct and an increased emphasis on corporate responsibility. These emerged in the aftermath of a period that saw a major shift in the economic role of the state, and in policies towards transnational corporations (TNCs) and foreign direct investment.[6] Codes of conduct in the copyright area emerged during the 90's and form the trend of the last decades.

In the Greek Copyright Law (Law 2121/1993) they are stated in article 66D bearing the title "Codes of Ethics and Information Exchange".[7] According to it, codes of conduct may be prepared by the business or professional associations concerned, as well as collecting societies or collective protection organizations, with respect to issues of copyright enforcement. This article also makes a direct reference to the use of codes in optical discs with the purpose to identify the origin of their manufacture; this, however, was inserted in the law in compliance with article 17 of the Enforcement Directive. The same article provides that codes of ethics and any evaluation of their implementation shall be forwarded to the European Commission, whilst the Hellenic Copyright Organization is designated as the national correspondent for such issues.

On a European Union level, two Directives make direct reference to codes of conduct. The E-Commerce Directive in article 16 (entitled 'Codes of Conduct')[8] provides that

"1. Member States and the Commission shall encourage:

(a) the drawing up of codes of conduct at Community level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of Articles 5 to 15;[9]

(b) the voluntary transmission of draft codes of conduct at national or Community level to the Commission;

(c) the accessibility of these codes of conduct in the Community languages by electronic means;

(d) the communication to the Member States and the Commission, by trade, professional and consumer associations or organisations, of their assessment of the application of their codes of conduct and their impact upon practices, habits or customs relating to electronic commerce;

(e) the drawing up of codes of conduct regarding the protection of minors and human dignity.

2. Member States and the Commission shall encourage the involvement of associations or organisations representing consumers in the drafting and implementation of codes of conduct affecting their interests and drawn up in accordance with para-

graph 1(a). Where appropriate, to take account of their specific needs, associations representing the visually impaired and disabled should be consulted."

The Enforcement Directive also contains provisions on codes of conduct.[10] In particular, article 17 entitled 'Codes of Conduct' provides that "*Member States shall encourage: (a) the development by trade or professional associations or organisations of codes of conduct at Community level aimed at contributing towards the enforcement of the intellectual property rights, particularly by recommending the use on optical discs of a code enabling the identification of the origin of their manufacture; (b) the submission to the Commission of draft codes of conduct at national and Community level and of any evaluations of the application of these codes of conduct*". Also in its Preamble in Recital 29 it provides that: "*Industry should take an active part in the fight against piracy and counterfeiting. The development of codes of conduct in the circles directly affected is a supplementary means of bolstering the regulatory framework. The Member States, in collaboration with the Commission, should encourage the development of codes of conduct in general.[...]*"

"Creative Content Online in Europe's Single Market" Communication also makes reference to codes of conduct.[11] In this Communication the Commission identifies four main, horizontal challenges which merit further action at EU-level, amongst which 'legal offers and piracy' are included. According to a press release, the Commission intends to instigate co-operation procedures ("codes of conduct") between access/service providers, right holders and consumers in order to ensure not only the widespread offer of attractive content online, but also adequate protection of copyrighted works, and close cooperation in the fight against piracy and unauthorised file-sharing.

### *Current Practice*

Since the interests concerning the Internet have developed and strengthened requiring a lot of time and energy on the part of the European Union to legislate, recourse to self-regulation solves many problems and takes the burden (political or other) away.

Codes of conduct dealing with copyright infringement on the Internet take different stances on the matter varying from notice and takedown procedures, graduated response models, termination of accounts, filtering and monitoring of traffic and communication data to mere warnings and procedures which allow ISPs to reveal subscribers' identities or introduce exceptions to the secrecy of communications to the same end.

Examples of such codes are as follows:

- Code of Practice and Code of Practices and Ethics that were adopted by the Internet Service Providers Association of UK[12] and Ireland in 1999 and 2002

respectively.[13] The Code of Conduct of India adopted by the Internet Service Providers Association of India should also be added to them.[14] These codes refer to good practices followed by ISPs on the Internet including decency, honesty, fair trading, data protection, privacy and so on.

- the Dutch Notice-and-Take-Down Code of Conduct, which was published in 2008.[15] The code is a voluntary agreement between Dutch internet service providers and government enforcement agencies and seeks to clarify the responsibilities of the former (hosting providers in particular) when confronted with situations relating to unlawful (under Dutch law) online information.

- A code of conduct for ISPs published jointly in 2005, by the International Federation of Phonographic Industries (IFPI) and the Motion Picture Association (MPA). This code provides for filtering technology to block services or sites that are substantially dedicated to illegal file sharing or download services. It also contains provisions which require subscribers to consent in advance to the disclosure of their identity in response to a reasonable complaint of intellectual property infringement by an established right holder defence organisation or by right holder(s) whose intellectual property is being infringed.[16]

- The Principles for User Generated Content Services, which was the outcome of an agreement between a number of major film producers with several large providers of user-generated content services (UGC) in the United States (2007) including MySpace and Dailymotion. This agreement obliged UGC service providers to cooperate with content owners on the use of content identification and filtering technologies.

- The Irish arrangement concluded in 2009 between the Irish Recorded Music Association (IRMA) and the telecommunications provider Eircom as a result of litigation concerning copyright infringement on the Internet.

- The YouTube Terms of Use, which basically repeat the US provisions on notice-and-take-down found in the Digital Millennium Copyright Act (DMCA).

- The Facebook's Statement of Rights and Responsibilities and the Terms of Service of the Google search engine that govern their relationship with their users and also refer to the US provisions on notice-and-take-down.

- The Code of Conduct of the Canadian Association of Internet Providers (CAIP).

- The Code of Practice in Australia published by the Internet Industry Association on cybersecurity.[17]

Codes of conduct present a number of advantages.

They come within the scope of soft law as a form of self-regulation or co-regulation. Self-regulation is when the stakeholders regulate for themselves (e.g. ISPs regulate for ISPs or ISPs and rightholders regulate for ISPs). Co-regulation is when the Government is involved in this procedure (usually under the threat of legislating) on its own initiative or under the pressure of the industry. This involvement can take many forms such as for example participation in the process towards the adoption of the rules or in the form of supervising the results of such a process. Codes of conduct (as a result of self-regulation or co-regulation) either replace or supplement the law. In this sense governments avoid to enact new laws which would cover the existing legislative gap or clarify ambiguous legal situations. That means that by codes of conduct governments save time, money and energy by sparing themselves the legislative process. On certain occasions, they also save the political debate which comes with it.

Codes can be drafted expediently and respond immediately to the problem at issue.

They are also flexible in the sense that they can be updated and easily changed in order to accommodate technological developments and social needs.

Codes of conduct also set norms in a low profile given the fact that they are voluntary schemes. That means they standardize a particular conduct in the area and open up the way for future legislation.

Given that the drafters are usually the interested parties (stakeholders), the solutions followed are usually very closely geared to the problem. That means that they can provide for fast and effective remedies (such as content removal or subscription termination), in fact a lot faster when compared to what a rightholder would have achieved through the courts even in summary proceedings or through an injunction. Such expedient remedies also work as an effective deterrent to would be infringers.

Last but not least, self-regulatory enforcement may be less costly compared to courts.

Codes of conduct come with a number of shortcomings, too.

The fact that they are drafted by the stakeholders themselves can work both as an advantage and as disadvantage. The advantage as described above refers to tailor made solutions. However, the parties involved in its drafting are not always all the parties affected by it, e.g. consumers or the public at large. In this sense one could argue that codes of conduct present a democratic deficit regarding participation and representation and are usually one-sided as they serve the interests of the drafting parties only. To this the lack of transparency could be added. The reality, however is that the codes of conduct may be more transparent than the law itself. This is so in cases where the law is drafted by the State itself without

the involvement of any of the parties concerned even more of any of the parties affected. In any case, a code of conduct can change far easier compared to law.

Also, the fact that codes cannot be enforced in the sense a legal provision can, since they do not provide for sanctions in the form a law does, presents a serious drawback[18]. A usual sanction is the dismissal of a member from the association which has adopted the code or the presumption that this particular member does not operate on high professional standards or follow good business practices. Dismissal is not a sanction *stricto sensu* but the pressure exercised on the dismissed member may, in some cases equal a proper sanction. Also the fact that sanctions are 'softer' compared to proper legal sanctions creates legal uncertainty.

Although codes of conduct are not binding for those who have adopted them they could however end up being binding for those mostly concerned. For example, ISR which are bound by such a code will usually reflect the terms of the code to their contracts with subscribers. In this way the norms of the code will end up as binding contractual provisions for the consumers. On top of it the respect of ISPs for the terms of a code of conduct may play a role towards the assessment of their liability in copyright infringement cases. In fact it is very likely that a Court will take into account in assessing whether an ISP has acted with due diligence or took any reasonable steps to prevent or avoid the doing of the act, whether it has acted within the standards accepted in the area as reflected in a code of conduct[19].

As regards costs, one may argue that costs are not always low. If one has to turn to the courts, the total costs of litigation on top of the costs of a first round of self -regulatory enforcement procedure will usually exceed those of litigation alone.

## Conclusions

Codes of conduct provide for a less intrusive solution which brings the various stakeholders together and gives them the opportunity to solve themselves the issues at stake. This can be done under the auspices of the State or without the State's involvement. It can also be argued that codes of conduct, though voluntary schemes, may in certain cases, form or transform ethics in the area or even operate (indirectly) on the same level as law. It is, however, both difficult and unrealistic to say whether codes of conduct provide a good or a bad solution to a problem. Their utility depends on the problem, the solution they are called to offer, and the timing. It also depends on whether they replace or supplement the law. The latter seems closer to their purpose and provides better guarantees for proportionality and respect for fundamental freedoms and rights.

As the European Commission sets out in its 2001 White Paper on European Governance, combining formal legislation with non-legislative and self-regulatory solutions

supports the clearer definition of EU policy objectives and improves the effectiveness of those policies.

## Endnotes

1. According to the EDPS Opinion, "The different on-line intermediaries can be defined according to their functional roles. However, in the real world intermediaries usually take on several of these functions. On-line intermediaries include: (a) *access providers:* users connect to the network by connecting to an access provider's server; (b) *network providers:* they provide the routers, *i.e.*, the needed technical facilities for the transmission of data; (c) *host providers:* they rent space on their server, upon which users or content providers can upload content. Users may upload and download material to an online service, such as a bulletin or a P2P networks", EDPS/10/3 Brussels, Monday 22 February 2010. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf, p. 4, ftnte 10.
2. Opinion of Advocate General Kokott in *Promusicae v. Telefonica* (C-275/06), [2008] ECR 271, as this Opinion was delivered on 18 July 2007, paras 30seq.
3. Silke von Lewinski, "Certain legal problems related to the making available of literary and artistic works and other protected subject matter through digital networks", (1.1.2005) prepared at the request of the UNESCO Secretariat for the 13th Session of the Intergovernmental Copyright Committee, 2005, <http://portal.unesco.org/culture/en/ev.php-URL_ID=27931&URL_DO=DO_TOPIC&URL_SECTION=201.html>.
4. A useful definition is provided in the 2007 International Good Practice Guidance, *Defining and Developing an Effective Code of Conduct for Organizations*, the International Federation of Accountants: "Principles, values, standards, or rules of behavior that guide the decisions, procedures and systems of an organization in a way that (a) contributes to the welfare of its key stakeholders, and (b) respects the rights of all constituents affected by its operations".
5. In the sense of a branch of philosophy which seeks to address questions about morality (i.e. what is good and bad, right and wrong, and so on.
6. Rhys Jenkins, "Corporate Codes of Conduct: Self-Regulation in a Global Economy", http://www.unrisd.org/unrisd/website/document.nsf/0/E3B3E78BAB9A886F80256B5E00344278?OpenDocument.
7. Article 66D: "(1) The business or professional associations concerned, as well as collecting societies or collective protection organizations, shall prepare codes of ethics with the purpose of contributing, at national, Community or global level, to the enforcement of the rights under this law and shall recommend the use of codes in optical discs in order to identify the origin of their manufacture. The codes of ethics and any evaluation of their implementation shall be forwarded to the European Commission. (2) The national correspondent for the rights under this law shall be the Hellenic Copyright Organization". This article was introduced by article 2 para 7 of Law 3524/2007 (FEK A' 15/26.1.2007).
8. 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*.

9. Articles 5 – 15 are the main provisions of the Directive, i.e. almost all Chapter II (except article 4) entitled 'Principles'.
10. 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 157/45, 30 April 2004 (Enforcement Directive).
11. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/5.
12. http://www.ispa.org.uk/about_us/page_16.html#Scope.
13. ISPAI Code of Practice and Ethics, available at www.ispai.ie/docs/cope.pdf.
14. http://www.ispai.in/codeOfConduct.php.
15. Notice-And-Take-Down Code of Conduct, drafted under the auspices of ISOC.nl, available at http://isoc.nl/info/nieuws/2008-noticeandtakedown.htm.
16. C. Arthur, 'IFPI Drafts 'Code of Conduct' for ISPs', *The Register*, 12 April 2005, <www.theregister.co.uk/2005/04/12/ifpi_drafts_code_of_conduct>.
17. Internet service providers voluntary code of practice for industry self-regulation in the area of cyber security, Internet Industry Association, http://iia.net.au/images/resources/pdf/icode-v1.pdf.
18. This is the reason why some countries such as France and the UK have opted for legislation. In particular, in France the HADOPI law was adopted providing for the suspension of Internet access in cases of repeated copyright infringements on the Internet (See Law No. 2009-669 of 12 Jun. 2009 favoring the diffusion and protection of creation on the Internet (Official Journal, 13 Jun. 2009) (HADOPI I) and Law No. 2009-1311 of 28 Oct. 2009 relating to the criminal protection of copyright on the Internet (Official Journal, 29 Oct. 2009) (HADOPI II). In the UK the Digital Economy Bill (now Act) was passed (9.4.2010) authorizing the suspension of internet service for those who repeatedly download copyrighted material illegally <http://www.publications.parliament.uk/pa/ld200910/ldbills/055/10055.1-6.html>.
19. For example, in a US case by the District Court in New York, YouTube was found to be covered by a 'safe harbour' clause in the Digital Millennium Copyright Act that protects ISPs from penalties for their users' copyright violations to the extent ISPs address those violations once they are made aware of them <http://malaysiandigest.com/world/37-world/8962-google-wins-youtube-copyright-case-in-spain-.html> (24 September 2010).

# On Formal Methodologies for Computer Supported Computer Ethics

**Petros Stefaneas**

## Introduction

Nowadays more than ever, computer ethics and information law are most helpful to the way we approach everyday applications. Stemming from this reality computer-supported computer ethics is a promising area for research. Still, the complexity of issues involved and the different problems addressed on each individual occasion make this task a hard one. In this short paper we argue in favor of the possible applications that formal methodologies may have on computer ethics. We claim that algebraic specification languages, such as CafeOBJ may be used to shed new light on the promising interaction between formal methods and computer ethics. A nice example is the application of CafeOBJ into OMA REL Licenses. OMA-Digital Rights Management System is a standard proposed by Open Mobile Alliance for protecting digital content distributed through mobile networks.

## Formal Methods

Formal Methods (FM) is an area in computer science, which uses techniques from mathematics and formal logic for the specification, design and verification of software and hardware systems. Typically, each formal method has its own semantics and depends on a particular logical system. Most of the formal methods can be implemented in a computer. The use of such methods entails the advantage that they guarantee higher levels of correctness. Formal Methods tools allow comprehensive analysis of requirements and design, and complete exploration of system behavior, including fault conditions. Z, OBJ, VDM, CASL, B-Method, CafeOBJ, Petri Nets are few of the best known formal methods. The benefits of using Formal Methods include:

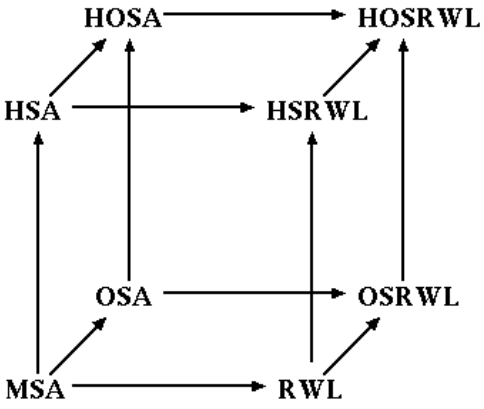
1) An objective measure of the correctness of a system, as opposed to current process quality measures.

2) Early detection of possible defects. The application of FM leads to early detection and elimination of design defects.

3) Guarantee of correctness. Unlike testing, formal methodologies and their tools consider all possible execution paths through the system.

An interesting formal method is CafeOBJ. This is an algebraic specification language/system, based on equational reasoning. It can be used to specify abstract machines as well as abstract data types. A visible sort denotes an abstract data type, while a hidden sort, the state space of an abstract machine. The CafeOBJ system rewrites a given term by regarding equations as left-to-right rewrite rules. An Observational Transition System, or OTS, is a kind of transition system that can be written in terms of equations in an algebraic specification language. We assume that there exists a universal state space called Y and we also suppose that each data type we need to use in the OTS, including the equivalence relationship for that data type, has been declared in advance.

The semantics of CafeOBJ uses more than one logical system, including equational logic, order sorted equational logic, hidden sorted equational logic, rewriting logic and their combinations. This can be nicely viewed in the following "CafeOBJ cube":




## Computer-Supported Computer Ethics

Privacy and data protection, intellectual property rights, computing at workplace, digital divide and social aspects of computing are some of the topics of computer ethics. So far, there many attempts to utilize computer programs and information systems to understand ethical issues. Historically, one of the first attempts to use computer programs for ethical issues was the well known program ELIZA written by Joseph Weizenbaum from MIT. ELIZA was a program making the computer act as a psychotherapist. Other programs can be mentioned also, such as these applied to computer-assisted game theory, applied cognitive science, AI and deontic reasoning.

## Formal Methodologies for Computer Supported Computer Ethics

In computer-supported computer ethics, formal methods can be used to provide a report on where inconsistencies lie. For verification, the input may be a specification and a desired ethical property of a system, and the output may be either "Yes, the property is valid" or "The property is not valid". Formal methodologies based on deontic logic provide a description and informal analysis of the commonalities in ethical discourse. For example, the logic model (DEAL) makes use of recent research in deontic, epistemic and action logic, and indicate - drawing on recent research in computer implementations of modal logic - how information systems that implement the proposed formalization may be developed [4]. Another interesting example is where mechanized multi-agent deontic logics are considered as the appropriate vehicle for engineering trustworthy robots. Mechanically checked proofs in such logics can serve to establish the permissibility (or obligatoriness) of agent actions, and such proofs, when translated into English, can also explain the rationale behind those actions. As formal method they use the theorem prover Athena in order to encode a natural deduction system for a deontic logic.

## A CafeOBJ formal specification

To demonstrate the usefulness of formal methods to address issues of computer-supported computer ethics we will present briefly a CafeOBJ specification related to Open Mobile Alliance for protecting digital content distributed through mobile networks. To address this problem an abstract syntax for OMA-REL and writes an algebraic specification of it using CafeOBJ is proposed, with future goal the creation of automated tools that check the behaviour of a set of licenses under a certain environment. In the following table we give the basic data types used and their corresponding modules.

| Data Types | CafeOBJ Modules |
|---|---|
| Sets | SET |
| Constraints | CONSTRAINT, INDIV, CONSTRAINT-SET, DATE, VERSION, SYSTEM, INTERV, SYSNAME, CONS |
| Actions | ACTION |
| Permissions | PERMISSION, PERMISSION-SET, PER, TOPPermission, TOPPermissionSET, TP, TOPPermission2, TP2 |
| Assets | ASSET |
| Uids | UID, UIDSET |
| Agreement | AGREEMENT, AGREEMENT2 |
| Allowed actions set | RESULTS, RESULT-SET |

| | |
|---|---|
| Function [[.]] | AGR-F, AGR-F2 |
| Data Types | CafeOBJ Modules |
| Sets | SET |
| Constraints | CONSTRAINT, INDIV, CONSTRAINT-SET, DATE, VERSION, SYSTEM, INTERV, SYSNAME, CONS |
| Actions | ACTION |
| Permissions | PERMISSION, PERMISSION-SET, PER, TOPPermission, TOPPermissionSET, TP, TOPPermission2, TP2 |
| Assets | ASSET |
| Uids | UID, UIDSET |
| Agreement | AGREEMENT, AGREEMENT2 |
| Allowed actions set | RESULTS, RESULT-SET |
| Function [[.]] | AGR-F, AGR-F2 |

The module used for the definition of constraints as an example and for better understanding of the specifications:

```
mod* CONS{
pr(CONSTRAINT-SET + NAT + INDIV + SYSTEM + DATE + INTERV)
op timeCount [ _ , _ ,_ ,_ ]: Nat Nat Nat Nat -> Cons
op count [_ , _]: Nat Nat -> Cons
op True: -> Cons
op accumulated [ _ , _ ]: Nat Nat -> Cons
op individual [_ , _]: Ind Ind -> Cons
op System [_ , _ ]: Sys Sys -> Cons
op datetime [ _ , _ ]: Dt Dt -> Cons
op interval [_]: Interv -> Cons }
```

## For Future Reference

Arkoudas, K. and Bringsjord, S. (2007). Computers, justification, and mathematical knowledge. Minds and Machines. vol. 17, no. 4, pp. 185-202.

Bringsjord, S., Arkoudas, K., and Bello, P. (2006). Toward a general logicist methodology for engineering ethically correct robots. IEEE Intelligent Systems, 21(4):1541–1672.

Goguen J., and Burstall R. (1992), Institutions: Abstract Model Theory for Specification and Programming, Journal of the Association for Computing Machinery, 39 (1): 95-146.

M. J. van den Hoven & G.J.C. Lokhorst. (2002). Deontic logic and computer-supported computer ethics. Metaphilosophy, 33 (3): 376-386.

James, H. F. (1988). Program verification: the very idea. Communications of the

ACM, 31(9):1048–1063.

Johnson, D. G. (2001). Computer Ethics. Prentice Hall, 3rd edition.

Pike, L. , and Abramson D. (2007). When formal systems kill: computer ethics and formal methods. North American Computers and Philosophy Conference (NA-CAP). Chicago, Illinois.

Danielson P. (1992), Artificial Morality: Virtuous robots for virtual games. Routledge, London.

Goldman A. Ethics and cognitive science. *Ethics* 103 (1993), pp. 337-360.

Castelfranchi C. Artificial Liars: Why computers will (necessarily) deceive us and each other. Ethics and Information Technology, vol. 2, no. 2 (2000), pp. 113-119.

Lee R. DX: A deontic expert system shell. EURIDIS internal report 92.10.01b, Erasmus University Rotterdam, 1992.

Tan Y-H. A logical model of trust in electronic commerce. Electronic Markets, vol. 10 (2000) pp. 258-263.

Triantafyllou N., Ouranos I., and Stefaneas P., Algebraic Specifications for OMA REL Licenses. WiMob 2009: 376-381.

# Privacy in libraries: the co-existence of ethical principles and legal rules

**Vassiliki Strakantouna**

## Introduction

The rapid development of information technology, the fast growth of networks and the transition of the internet from web1 to web2, form the new digital information environment. The production of information in electronic form is continuously increasing, the speed of information processing through the computer is being multiplied, the cost of archiving is being decreased and the internet services are spreading to a wider specter of people and social activities. The nature of information changes as it converts to a marketable good of additional economic value. New technologies and digital means aid to collect data from different sources faster, the match of those is easier to achieve, and in the same way, the recombination of new information with negative effect on individual's rights and freedom, becomes possible.

The deployment of new technologies in libraries, the sophistication of modern automatic systems that they adopt, the sharp increase of the amount of information that they process but also, the increasing interest of exogenous factors as for the libraries, for search and abuse of their archives, form an upcoming fear for the users' violation of privacy of library's services. At the current information environment new services and management tools, coexist with old techniques and practices, habits and values, which sometimes make obvious and painful the incapacity of handling the new and different one. Caution, on the part of the librarians and other information professionals as for how the old and sometimes intuitive habits of evaluation or the close interpretation, are enough and suitable in the "new worlds", the new and different situations that are being formed by the integrated library systems. Legal and ethical principles, challenges and dilemmas for the protection of individual rights and especially for the protection of personal data, intellectual property, freedom of information, freedom of expression, are issues for the moment in librarianship.

In the context of this presentation, the examination of the parameters of privacy and protection of personal data in libraries will take place. Special emphasis will be given to the exploration of the possibility for the creation of a self-regulatory framework of protection and the power of libraries or the professional union to

establish rules and what force and binding can these rules have, especially when it concerns to individual rights which are followed by a necessary regulatory intervention by law. Finally, the proposal of a professional code of ethics for the protection of personal data in libraries will be presented.

## The protection of privacy from the collection and processing of personal data in libraries

Libraries, the depositories of human knowledge, the past, the present, and our future, "the memory of humanity", play a very important role to the examination and the facilitation of access to the constantly increasing number of local and remote information resources and services. Apparently from their nature and their particular goals, libraries have the user or the patron as a main target, aimining at their satisfaction of special needs for research and use of demented information. Rules, regulations and technologies are used, in an attempt to give access to services and resources, with no unreasonable restrictions, with respect to patrons' individual rights.

The right to privacy is the right of everybody to form his life according to his beliefs, anonymously, undisturbed from foreign interventions. This right provides the individual with the power to forbid others to abuse his personal space and his anonymity. The protection of privacy or personal life is supported by the whole librarians' community in theoretical as well as in practical level. In texts of the American Library Association (ALA), the specialization and the clear distinction of the terms privacy and confidentiality are observed[1]. The right to privacy in the context of libraries means the right of free search of information without the user's reading choices to be examined or censored. The right to confidentiality, also, means the obligation of the library not to notify others of the user's personal information that may have at its disposal. Librarians recognize that privacy is essential to the exercise of free speech, free thought, and free association and therefore, essential to democracy (Adams, H. [et al.] 2005 and Bottis 2006).

Libraries collect and edit personal information and personal data in order to provide services to their patrons, for better and more effective information management, and development of their services. This era in which libraries and their users are now struggling, is different in one way from any other period in human history. Never before has it been possible to gather such vast quantities of personal information, and bring it all together to create a detailed profile of each and every individual (Woodward J, 2007). Competition, upgrade, and automation of the functions and services, has led to the adoption of new technologies and digital tools, such as technologies for the identification of users through Radio Frequency Identification (RFID) or biometrics, the adaptation of web2 technologies (Blogs, RSS Feeds, Facebook, Twitter, Flicker etc), which lurk new risks.

In the new digital information environment, the recordings of acts and moves of the users are constantly growing and there is a wider and easier access to the relevant archives that become more, and more comprehensive and easier to use. The access to electronic resources demands the definition of the users' identities. The mediation of Internet Service Providers raises issues in relation to storage, possession and use of personal data of those who use these services. The services of digital libraries and the creation of personalized and customized environment according to user's preferences, demand the collection of more and more personal information.

Public websites and especially Facebook are used by libraries and librarians as a tool in order to communicate with professionals of the same scientific field and to notify a library's activities or facts. Also, many facebook applications for libraries have been developed (Facebook Group about Library). As the use of facebook creates complete digital profiles of the users, deep concern is observed in the collection of such great amount of personal data by Facebook Inc, the possibility of their processing by the same company or other associated companies and the risk of state authorities to use them as a means of surveillance. The company has the ability to share users' data to others in some cases that is considered to be necessary for some reasons (service offer etc). The company can also share information when necessary for the satisfaction of any obligations imposed by law or for the deterrence of web-crime. Furthermore, every registered friend is able to copy, edit, change and re-publish data (Piskopani, A-M, 2009).

In the library world, RFID tags, replace the technology of barcodes on books and other items in order to achieve a more productive and more improved library's collection management. The reason why the critics of this technology are concerned is that the growing risk for privacy of record borrowers from libraries, because of the amount of data and the limited security of these systems (ALA, RFID).The use of RFID tags has raised also privacy issues centered on concerns that the technology will make it easy to detect what patrons have checked out from the library. According to Butter there are threats that refer not only to the borrower or the debtor, but also to the collection of the library (Butters 2007).

The violation of privacy referring to the undesirable processing of personal data is stemming not only from the possibility to edit archives with personal data that create and maintain libraries themselves, but also, from he possibility for exploitation data that third parties might have leveraging on the data activities regarding access and use of library's services offered in electronic format and/or in the online environment of the internet The appropriate processing of all these archives gives the opportunity to form an "invisible image" of users, as it can reveal values, political and religious beliefs, research interests, consumers' preferences,

health problems etc. It is worth mentioning that in many cases, researches and reading preferences reveal data that the law considers as "sensitive", by reserving essential, enhanced and procedural protection.

The main risk for these personal data is to be used for a different cause than the one for which they were collected. In the context of libraries, many institutions with different purposes are interested and sometimes press for the acquisition of access to archives that reveal the preferences of library users. These institutions are a) private such as database providers that are interested in the check of database use, commercial companies that want to promote products, publishers and bookstores that want to know the reading trends or habits of the users etc., and b) public institutions, mainly prosecuting authorities that seek access to readers' archives so as to use them for national security and crime detection reasons. In U.S libraries, for example, privacy of users has many times been violated when the prosecuting authorities asked for the use of library archives in order to detect crimes, even though the strong resistance of the library community. A common example is the American authorities' demand to access archives with personal data and reading habits of users in order to find those who were responsible for the terrorist attacks of the 11th of September ((Gardner, 2002), (Weiner, 1997). Estabrook, 2003).

The use of personal data for different reasons, challenges a basic principle of the data protection legislation i.e., the "purpose principle" and the associated prohibition of secondary use of data, which is based on national and international regulatory texts. The "purpose principle" is based on the article 5 of the Convention 108 of the European Council, on the article 6 of the instruction 95/46EK of the European Parliament and the Board of 24th of October 1995, on the article 8 of the Map of Fundamental Rights of the European Union and the article 4 of the Greek law 2472/1997. Additionally, with the reserve of exceptionally achievement of the superior public interest or legal interest of third person, disposal, notification, and transmission of personal data challenges, first of all, the right of people's informational self-determination, which means the right of the data subjects to determine which information that concerns them will become known to others and who will be the receivers of this information.(Strakantouna V...[et al.] 2007).

The uncertainty concerning to the use of personal data in the field of libraries is possible to have a significant negative impacton the relation between the user and the library. If habitual users believe that their privacy is threatened, they will limit their access to the facilities, services or the informational recourses so as to protect themselves. This will result in an irreversible damage of the public's trust to libraries regarded to be considered as "safeguarding sites" of privacy and

free research of knowledge but places where the reading choices will be notified, checked and judged by others.

## Law and ethics for the protection of privacy in Libraries

Users, in order to satisfy their informational needs, turn to libraries because of their reliability to the given services and because they are thought to be legitimate collectors of users' right of information and right to privacy. It is supported that information professionals are not enough to protect alone these rights (Sturges P., 2002).

The respect to these rights is simultaneously a legal and ethical obligation of both libraries and librarians. In Greek Law the right of information is guaranteed by article 5, paragraph 1 of the Constitution of Greece. This is the right of research, collection and reception of information but also the right to access a pluralistic frame of information sources. This right is limited according to article 5A, paragraph 1, only for national security reasons, for crime fighting or protection of rights and interests of others. By interpreting this article in the framework of the function of libraries, the information professional cannot limit unreasonably the right of the user to have access to the informative material of a library. The access to library information is guaranteed by the Constitution of Greece and especially the article 16 1975/86/01, according to which, freedom of science and especially freedom of accessing the conclusions of searches and generally the public accessible inquiring elements. The obligation of libraries to ensure the access of users to any kind of knowledge and information specialized and to the "Regulation of Library's Operation" (YA 8300/2003) which contains regulations for the operation of libraries and certain ethical rules (Kanellopoulou-Bottis, M, 2004).

Contrary, neither the "Regulation of Library's Operation" nor the relative law about libraries (L. 3149/2003 (FEK A' 141) "National Library, Public Libraries and other provisions"……), contemplate a special obligation of information professionals to protect patron personal data and privacy. However, the right of protecting personal data is explicitly guaranteed in the new article 9A of the Constitution of Greece 1975/1986/2001. Specific legislation which has as a base the law 2472/1997 for the "protection of the individual from the processing of data of personal character", who was banned from law 3471/2006 to embody the direction 97/66/EC that was also banned by 2002/58/EC which provides a series of principles and rules that have to be followed by the "managers of processing" of personal data.

The obligation of librarians and other information professionals to protect patron rights is found in many deontological or ethical codes. It is meant that professionals are obliged to the society to have a specific behavior, by supporting the

basic principles of its professional terror (Rubin, 2000). Deontological rules have to do with the sense of ethics so that deontology is considered as an expression of ethics. Ethics is a source of inspiration of the basic principles of deontology, such as the duty of information, equal treatment and respect of personal life is ethics. Code of ethics or codes of conduct or best practices have usually the form of a list of ethical duties that professionals of every department have to fulfill, according to the characteristics and their capacities, independently from their obligations as they are formed by law. The principles of such codes are dictated from an ethical system which defines the limits within which professionals can work, act and regulate the behavior and the permitted methods during the exercise of their professional duties. They set out the requirements of ensuring quality services and may be found as beneficial mechanisms so as to improve the standards of a professional terror and useful at the regulation of an ethical frame for its professionals. A main characteristic of such codes is that they do not -legally-have a compulsory nature and are revised every time that the circumstances require or justify it (Livada Chr, 2005).

In the era of a digital technology, professional ethics of information scientists are considered very important issue because of the new risks for the protection of personal data and intellectual property. Information ethics is a constantly evolving field of research and demands a scientific approach. The new code of ethics includes individual issues, set principles and suggest practises that make the flow of information and ideas easier, protect and promote the rights of every person in free and equal access in information sources. Lately there has been discussions upon the issues of equal access to information sources from an ethical and deontological point of view, at least more discussions then ever before in the librarian context.

The greatness of ethical and deontological codes in the daily practise of librarians and other information professionals is widely accepted and the development and promotion of the codes of professional behaviour is a matter that concerns the professionals since the 19$^{th}$ century. A series of recent codes for librarians is found in the website of IFLA (IFLA FAIFE). For the structure and organization of the content in many of them is used the user/profession/collection approach, placing great emphasis on the respect of users' rights, the social mission of the profession, the duties and rights of professionals, the development and maintenance of collections according to the users' needs and the role of libraries in each community (Sturges, 2009). Principles and values like protection of privacy, protection of intellectual property and resistance to censorship, equality of treatment among users, universal access to the internet, freedom of expression, freedom of knowledge, support of open and free access to information, which are required in deontological codes or information policies for organizations and associations in

the wider field of informational science. The necessity and the usefulness of such codes are also noted by the national and European Community legislature, which instructs to the principle of personal data protection of every country, to urge the professional associations to institute ethical rules.

Despite the establishment of code of ethics, many professionals wonder about their usefulness, especially when through them is attempted effort to regulate individual rights the regulation of which requires the regulatory intervention of law. The answer to this question will emerge from the examination of capacities and jurisdiction that a professional association or an organization has to regulate rules for the protection of rights but also of the nature of law that protects these specific rights. Moreover, it is quite useful to observe the way of regulating such issues in the wider environment of information, like the internet.

A professional association or an informational organisation like a library can introduce or establish code of ethics that regulate the relations between professionals and patrons (like the obligation of mutual respect and cooperation). The ability of them to establish rules for the protection patron's individual rights is being questioned. Their main argument concerns their legalization, since society has entrusted the evaluations of the individual rights to the state and not to the professional sectors. The regulation of individual rights is assigned to the State; the regulatory intervention of law is necessary and ethical rules are not sufficient. As the law of personal data protection is a complex but also a general system of principles, guarantees and rights, the expedient application of these rules depends on the ability to be adjusted to the needs of each environment and regulate it satisfactorily. This involves the specialization of general rules from the professionals. The law sets principles and every professional sector specifies the legislative needs.(Strakantouna V. [et al.] 2007). Especially as far as it concerns the specialization and adaptation to the library and information services context, the cooperation of information professionals is required, who, due to their specialization, experience, closer relation with their profession and their contact with technological development at the domain of librarianship and knowledge management, they are considered as more appropriate to predict the dangers for users and disincline them. Also, effective protection of library users depends to a great extent on the knowledge of protection need and the awareness not only of librarians and other information professionals but also of the subjects of personal information.

The regulation of privacy issues in digital era constitutes a complex matter, while the discussion about the most suitable frame of regulation is constantly developing. Apparently from legislating rules, the regulation of conflicts that human behavior creates is tested through self-regulation and the creation of ethical and

deontological rules. Methods that existed before the new technologies are kept and tested as a way of regulating in the internet and in the so-called highways of information, as self-governance. Globalization, the judgement of law and institutions, the emphasis on economic parameters of law and the problems of modern economy, created the presuppositions for the creation of a deregulatory environment. Overcoming the weaknesses of the traditional legislating regulation but also the problems created in the domain of self-regulation, is sought now in the model of co-regulation or controlled self-regulation which concerns the introduction and adoption of processes of consultation with those interested but also the experts (institutions, special scientists, citizens). It is about processes that help with the definition of tensions and the production of consent among the participants, which do not strictly lead to the production of law, but create a common space of dialog among the interested. In this model, the main regulator is the state, which defines the basic principles and the standards that must be in effect. Its role is found in the check of context of the rules and functions as a guarantor of the correct work of the production mechanisms of these rules (Mitrou, 2005). Thus, the state is not exhausting itself with the creation and the enforcement of impositions and prohibitions, but contributes to the aid of social institutions

In this frame, legislation has to consider the special role of libraries in social development, by predicting regulations that serve the wholeness, and the scientific associations have to promote the application of legal codes of ethic. This regulating model is followed by many attempts to create codes of practices, offering to professionals, principle guidelines which are specialized, in order to be applied in specific circumstances such as when interests are being jeopardized or confront other obligations, organisational structures and public safety. As far as the protection of personal data is concerned the Data Protection Code of Practice for the Higher and Further Education Sectors is very significant, with the support of Joint Information Systems Committee ASSIST (JISC 2002). Additionally, the Advisory Committee on Access to Information Systems and Services (ACAISS), of Society of College, National and University Libraries (SCONUL) has drawn up and published a relevant directory, in which the protection practices that are used in many British Colleges are mentioned. Its contribution is very important as it provides advisable acts for the treatment of subjects that have to do with the protection of personal data (Sconul 2002).

## Codes of ethics for the protection of personal data in libraries and information services

As far as the Greek reality is concerned, an attempt for the creation of a code of ethics for the protection of personal data was made by the author hereto in 2005. The suggestion of this code is a part of a postgraduate work with the title “process

of personal data and protection of privacy in the modern environment of libraries and information services" that was placed in discussion at the 14th Conference of Greek Academic Libraries in 2007.

This code emerged from the need for existence of a protective tool of personal data in Greek libraries, which was a result of the research that took place in 2005 in a typical example of Greek libraries. The purpose of this research was to seek a) the existence of policies that protect privacy in libraries, b) to what extent personal data is edited, c) the practises of collection, storage and availability of data, d) the level of concern of the personnel and users, e) the awareness of the existing legislation of the protection of personal data, f) the disclosure of cases of undesirable processing and the users' and personnel's reactions, g) the necessity of creating documents – instructions of the policies of privacy and protection of personal data.

The research revealed that all libraries create electronic archives with users' personal data. There are archives that contain a) users' information that is very important for the facilitation of functions and procedures, such as material movement, lending among libraries, use of electronic sources and databases, b) demands of members and external users for the information services and for specialized services, selective dissemination of information etc, c) members' and personnel's information, which emerge from the use of internal and external e-mails, d) recordings of online searches and other online activities that take place by the personnel's terminal or public use terminal, e) personnel's information for the fulfilment of economic and other demands and finally, f) recordings of information from the archives of the supervising and material handling systems and facilities. Comparing the 2005 results with the current situation we could say that libraries and their patrons are more informed about the risks that exist and therefore more careful, even though they continue to trust libraries but not the internet service providers (ISPs). Also in the most libraries websites you can see a privacy policy statement.

The above mentioned code of ethics for the protection of personal data in libraries and information services is an attempt to combine the self-regulating dynamic of the librarian practices and the regulatory rules of the Greek and European law about the protection of individuals with regard to the processing of personal data. The nature of these rules is dual. They are rules with committing and ratifying character that specialize in the current law of protection of personal data. Simultaneously, are simplified rules with explicit directions for the processing of personal data in libraries, that akin to ethical rules. As for its structure, firstly, the used terms of protection of personal data are clarified and specialized in the environment of libraries and information services.. According to the protection of

personal data policies when information is collected for the purposes of libraries' operation, from which we define the natural person, the library is considered by law as the "process manager" and librarians that collect data in favour of the information organisation as "processors". The library and its personnel, as "process manager", have to follow specific principles and rules for the process of personal data. The main body of the code consists of the following rules and principles which all users (personnel and patrons) have to abide with.

- The principles of fair and legal collection and process of personal data, which are applied independently from the data processing form and the ownership of libraries and information services.
- The general obligations of the library (to comply with legislation, adaptation to technology development, creation of policies, taking up legal competence, security mechanisms, education of personnel and users, providing the appropriate environment, delineating external requirements)
- The general rights of the subjects of data so as to be informed as for the capability of practice of their legal rights for information, accessibility, objection and temporary judicial protection.
- The specific commitments and demands of the library as for the organization of the archive system and the knowledge of its formation.
- The legal principles of the collection and process of data, users', personnel's, following the principles of proportionality and clarity purposes.
- The principles that have to be followed in case of the demand of others to access the archives, interconnection, maintenance and notification of data
- The principles of security and secrecy of data and process of processing manager, the administrators and the whole personnel.

Review and development of the suggested code according to the recent facts both in legislation level and in structural and context level so as to prevent new challenges and risks for the ones involved in the work of libraries, is indispensable.

## Conclusion

The right of privacy in the use of a library's services and resources will remain of paramount importance to the library profession. Librarians have a professional commitment to privacy, whether their libraries are located in a physical place or in cyberspace. Nowadays, privacy protection becomes even more difficult as personal data collected, processed and maintained easily but so much with difficulty we develop methods for their removal from the computer systems. Even though library users believe that their privacy is not threatened in the library, profession-

als owe to deter the risks, inform and train the personnel and the users accordingly to the value of privacy, by ensuring the appropriate frame of information handling, creating policies and tools of ensuring their individual and public rights.

## Endnotes

1. In a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf LA, An Interpretation of the Library Bill of Rights.

## References

Adams H, Bocher R., Gordon C & Berry-Kessler E. (2005) Privacy in the 21st century: issues for public, school, and academic libraries

ALA, An Interpretation of the Library Bill of Rights, http://www.ala.org/ala/issuesadvocacy/intfreedom/librarybill/interpretations/default.cfm, last access June 5, 2010

ALA, Radio Frequency Identification Technology http://www.ala.org/ala/aboutala/offices/oif/ifissues/rfid.cfm\, last access June 5, 2010

Butters A (2007) RFID systems, standard and privacy within libraries "The electronic Library vol. 25 No, 4, 2007

Bottis M. (2004) Information Law, Nomiki Vivliothiki (in Greek)

Bottis M., Privacy Protection in Information Services, DiMME 2008, 1, pp. 23-35 (in Greek).

Bottis M., Internet libraries and privacy, TEKMIRION, 2006, pp. 9-27, (in Greek).

Geraris, C. (2010) Personal data and new challenges DIMEE 1/2010 p. 42

Estabrook L.S. et al, (2003), Public Libraries' Response to the Events of September 11th. http://lrc.lis.uiuc.edu/web/911.html, last access June 5, 2010

Facebook Group about Library http://www.facebook.com/group.php?gid=2469777131, last access June 5, 2010

Gardner, C., (2002) Fact act or fiction: privacy in American Libraries, Proceedings of 12th Conference of Freedoms and Privacy, pp1-5 http://www.cfp2002.org/proceedings/proceedings/gardner.pdf, last access June 5, 2010

JISC (2002), Data Protection Code of Practice for the HE and FE Sections, http://www.jisclegal.ac.uk/dataprotection/DataProtectionLinks.htm, last access June 5, 2010

IFLA http://www.ifla.org/faife/ethics/codes, last access June 5, 2010

Livada, C. (2005) Codes of conduct in the financial sector: legal nature and function, Studies in Commercial and Maritime Law 32, A. Sakkoulas

Mitrou L. (2002) The Law in the Information Society, Sakkoulas (in Greek)

Mitrou L. et al. (2005) Self-regulation in Cyberspace, Sakkoulas (in Greek)

Piskopani A. M (2009) The protection of privacy in Facebook, DIMEE, 3, 350 (in Greek)

Rubin, R.E., (2004) Foundations of Library and Information Science, Neil Schuman

Karen Senior for the Advisory Committee on Access to Information Systems and Services of SCONUL . http://www.sconul.ac.uk/groups/access/papers/dpa_checklist.doc, last access June 5, 2010

Strakantouna V. (2005) Personal data processing and protection of privacy in the new frame of libraries and information services, http://dlib.ionio.gr/mtheses/vstrakan.pdf, last access June 5, 2010 (in Greek)

Strakantouna V., Piskopani A.M. & Mitrou L. (2007) Personal Data and Libraries, Chronika Idiotikou Dikaiou, (Z), 281-288 (in Greek)

Sturges P., Teng V., & Iliffe, U. (2001) User privacy in the digital library environment: a matter of concern for information professionals, Library Management, vol. 22, iss. 8/9, 364 - 370

Sturges P. (2009) Information ethics in the twenty first century, Australian Academic and Research Libraries, vol. 40 n. 4, 241- 251, last access June 5, 2010

Weiner, R. G. (1997) Privacy and Librarians: An Overview, Texas Library Journal 73(1) Spring, http://www.txla.org/pubs/tlj-1q97/privacy.html, last access June 5, 2010

Woodward J. (2007) What every librarian should know about electronic privacy, Libraries Unlimited

# Google's legal adventures and their impact to the evolution of European information law

Tatiana-Eleni Synodinou

## Introduction

On May 25th, Google announced its plan to launch a TV channel (the so-called Google TV channel). This spectacular decision is the last demonstration of the leading company's will to expand its activities to a wide scale of products and services[1]. Google has ceased to be a simple search engine; the company's multiple investments reflect a clear business strategy: to be present and even to dominate various branches of the IT industry.

Google's activities often appear to be highly controversial from a legal standpoint since Google seems to try to impose its ambitious business model without taking seriously into account restrictions established by law. Therefore, it is not surprising that Google's activity gave birth to a great number of litigations and to rich case law all over the world.

Google's business model is marked by the popular and misleading dogma that everything is permitted in Internet. This radical view is often expressed by the imposition of opt-out business models as regards the exercise of rights of third parties which are affected by Google's activities. The focal question raised is whether Google's multiple judicial adventures promote an evolution to law that reflects Google's business strategy or whether the IT giant will have to fully respect the European legal framework and legal culture and, as a result, to adapt its business model to constraints provided by law.

This paper will try to give an overview of the major legal questions which emerge from Google' dynamic presence in the Web. It is divided in four parts. The first part deals with the privacy implications which are born by Google's various activities, primarily by its main function as a search engine, but also by more sophisticated tools, such as the Google Street View service. The second part presents the basic copyright and trademark issues which have been raised by Google's services, such as the popular Google Library project, the Google news aggregator and its principal source of income, the Google Adwords service. The third and the fourth part focus on two relatively new fields of litigation: the eventual liability of Google for civil tort due to its Google's Suggest auto-completion search tool and competition law issues, such as the problematic of potential abuse of Goog-

le's dominant position in the European market of search engine providers for the low ranking of the Websites of its competitors.

## Google's leading business model and its privacy complications

Since Google's services depend on the collection and storage of a great mass of data, Google's technological breakthroughs are often considered as a threat for privacy. In February 2003, Google Watch nominated Google for a Big Brother Award, describing Google as a "privacy time bomb"[2].

Privacy implications of Google's activities have occupied several times the European privacy authorities. Indeed, the Article 29 Data Working party[3] in a number of occasions firmly expressed the view that the processing and the retention of personal data by Google in its primary function as a search engine but also in its ancillary activities raise a bundle of significant privacy concerns for European citizens. As it is going to be demonstrated in the following paragraphs, the European data protection legal framework seems to have influenced Google's privacy threatening tactics. The Article 29 Working Party has repeatedly marked the significant privacy implications of various Google's services and put some limits to the company's strategy to link its commercial success with an extended and often opaque processing of personal data.

### *The Google's search engine under privacy scrutiny*

The retention period of the search queries and their anonymization in the server logs was one of the first issues which were pinpointed as privacy concerning by the Article 29 Working Party[4] . In its Opinion 1/2008 on data protection issues related to the search engines[5], the Working Party distinguishes two different roles played by search engine providers with regard to personal data. First, in their role as service providers to the users, search engines collect and process vast amounts of user data, including, such as log files, IP addresses and cookies. Second, in their role as content providers, by retrieving and grouping widespread information of various types about a single person, search engines can create a new picture, with a much higher risk to the data subject than if each item of data posted on the internet remained separate.

According to the Opinion 1/2008, the Data Protection Directive 95/46 generally applies to the processing of personal data by search engines, even when their headquarters are outside the EEA, such as Google. Consequently, Google has to comply with the stringent data protection regime which is set up by the Directive in case it can be considered not as a simple intermediary but as a data controller[6]. The storage and processing of data has to respect the principle of lawfulness of the processing (article 6 of the Directive) and therefore search engines have

to specify explicit and legitimate purposes for which they process personal data. While the process of personal data could be made on the grounds of the user's consent or on the grounds that it is necessary for the performance of a contract, such as in case of registered services (e.g. a creation of a Gmail account), it is more delicate to evaluate when the processing is necessary for the purposes of a legitimate interest pursued by the search engine[7]. Legitimate purposes, such as services improvement, system security, fraud prevention or law enforcement have to be cautiously scrutinized in order to guarantee that the processing of users data is necessary and adequate and that the period of their retention is not excessive[8]. Moreover, the onus is on search engines in this position to clarify their role in the European Economic Area and the scope of their responsibilities under the Directive.

On the other hand, the e-Privacy Directive 2002/58[9] and the Data Retention Directive 2006/24/EC[10] are clearly highlighted as in general not applicable to search engine providers, because they fall outside of the scope of the definition of electronic communication services provided by the Framework Directive 2002/21/EC[11]. However, Directives 2002/58 and 2006/24 could still apply for additional services provided by search engines, such as the "Gmail" email service. Moreover, certain provisions of the e-Privacy Directive such as Article 5(3)(cookies and spyware) and Article 13 (unsolicited communications) are general provisions which are applicable not only to the electronic communication services but also to any other services when these techniques are used[12].

At this point it is worth mentioning that recently Google's social networking service "Buzz", which is part of Google's Gmail service, has been accused for privacy and consumer law violations in the U.S. The feature that attracted the biggest outcry was one which automatically gave users a ready-made circle of friends to follow based on the people they emailed the most. That meant the list of contacts was open for all to see and could have had serious privacy implications. After the protestations of privacy advocates, such as the Electronic Privacy Information Centre (EPIC), Google's engineers have now replaced the auto-follow feature with one that suggests who to follow but EPIC said that still leaves the "user with the burden to block those unwanted followers"[13].

In response to the Article 29 Working Party's Opinion, Google publicly announced its will to "anonymize" IP addresses in its server logs after 9 months[14]. Nevertheless, in its letter dated May 26, 2010, the Article 29 Working Party considered as insufficient the measure of deleting the last octet of the IP-addresses in order to guarantee adequate anonymisation and insisted that the data retention period should be further reduced to six months. Additionally, the Working Party urged Google to adopt supplementary measures in order to comply with the Eu-

ropean data protection legal framework. These measures include a reduction of the possibility to identify users in the search logs and the creation of an external audit process to reassure users that Google delivers on its privacy promises, i.e. by involving an independent and external auditing entity.

### *The "Google Street View" privacy threat*

Another delicate privacy concerning subject on EU privacy authorities is the potential risks posed by "panoramic street-level view services, such as the famous and successful Google's Street View. Street View was launched as part of Google Maps in May 2007 in San Francisco and has expanded rapidly since. What makes Street View truly unprecedented is the amount and density of consistent, geopositioned imagery it makes available to users[15].

According to a press release issued by the Article 29 Working Party[16], Google Street View raises serious privacy and data protection concerns. Even if Google blurs faces, car plates and other features that could allow the identification of people, problems could still arise from the storage and the eventual correlation of the vast amount of pictures required to enable the service and which Google has already collected. Notably, in 2009 Google Street view was prohibited by the Greek Data Protection Authority[17].

In February 2010, the Article 29 Data Working Party sent a letter to Google where it expressed its deep concerns about Google street view's practice to retain unblured copies of the images for one year and asked Google to alert residences in advance about the arrival of their Street View camera car. Apart from the eventual identification of persons and private houses[18] whose images have been captured by Google cars, other privacy complications comprise the capture of images in places which are "sensitive" from a data protection view (such as churches, hospitals, prostitution houses etc), the application of the principle of proportionality to the retention period of unblured images and the guarantee of the proper and effective exercise of the rights of the data subject, such as the right of information or the opposition right.

Another Google major privacy "sin" directly linked to its famous Street View service has been revealed recently. In May 2010, Google admitted in an official blog post that since 2006 it had mistakenly been collecting personal data from non-password protected Wi-Fi networks in more than 30 countries with its Street View cars. Indeed, Google collected about 600 gigabytes of data from users of public Wifi stations (which are not owned by Google) during 2006-2010, including snippets of emails[19]. Google issued a public apology and declared that it plans to delete all data as soon as it gains clearance from government authorities.

## Google in the vortex of intellectual property law

Google's ambition to become a leading information provider often appears to push European intellectual property law boundaries to their edges. This is demonstrated by a series of significant cases where the legitimacy of Google's innovative services such as Google news, Google cache, Google books and the major source of the company's income, Google Adwords, was thoroughly examined by European courts. While in the field of European copyright law, the underlying tendency is to strictly ascertain copyright infringement even in cases where in the US the fair use defense could have been applied. Concerning the thorny question of trademark infringement, the recent decision of the ECJ has been clearly marked by a more liberal approach which at least *prima facie* seems to comfort Google's leading advertising business model.

### *The Belgian "Google news" case*

Google's plan to conquer the Internet information market has been seriously tested in front of Belgian courts in the famous "Google News" case. In 2006 Google launched its Google News service, which is an automated news aggregator. The service covers news articles appearing within the past 30 days on various news websites. Its front page provides roughly the first 200 characters of the article and a link to its larger content[20]. When an article is still on line on the Website of its original source, Google redirects directly the user via the mechanism of deep links towards the page of the news website where the article is posted. Nonetheless, as soon as an article is no longer available in the news website, it is still possible to access its contents via a "cached" link which provides access to the contents of the article that Google are stored in the Google's system cache[21].

The Belgian press editors collecting society Copiepresse sought a prohibitory injunction against Google in 2006 for having stored, reproduced, extracted and reused without permission from the Belgian press editors the Belgian newspapers contents in its "Google News" daily press review. Copiepresse contested the legality of Google news service on the grounds of Belgian copyright law and of the database *sui generis* right[22]. Especially as regards the "Google cache" function, Copiepresse argued that the use of the "Google cache" makes it possible to circumvent the registration required by the press editor and, as a result, to elude the payment of the press article. Indeed, "caching" would make it possible to reach content that, the day after the event, is otherwise locked by the newspapers and subject to access fees[23].

The President of the Brussels First Instance Court firstly concluded that "Google news" does not function as a simple search engine but as an on line information

portal and that the use of "Google News" circumvented advertising on the websites of the newspapers which receive important revenues from advertising inserts. The President of the Court further noticed that the information was extracted from the press web servers without permission, and held that Google could not exercise any exception provided in the laws relating to copyright and neighbouring rights (Act of 1994) and in the law on database right (Act of 1998). [24]

The Court condemned Google for both copyright and database *sui generis* right infringement in September 5th, 2006 [25]. On February the 13th, 2007 the Belgian Court reaffirmed its original decision at least on the part that concerned copyright infringement[26]. Nevertheless, the question of copyright infringement due to the unauthorized reproduction of copyright protected works by Google's cached links seems to be still open in Europe. At this point, of major importance is the decision of September 17th, 2008 of the Provincial Court Barcelona (Audiencia Provincial Barcelona)[27]. The Court found that neither the unauthorized reproduction and display of fragments of web pages contents under the links that result from the Google search engine, nor the unauthorized reproduction and making available of the whole contents of web pages under the "Google Cache service" (different from the temporary copies made for proxy caching purposes[28]) constitute a copyright infringement. The Court grounded the exemption of Google cache on a flexible application of the three-step test[29] by using interpretative criteria comparable to the terms of the US fair use defense[30].

### *The "Google books" challenge*

Another legal battlefield for Google has proved to be its famous Library Project. Under the Library project, Google plans to scan into its search database materials from major research libraries all over the world. In response to search queries, users will be able to browse the full text of public domain materials, but only a few sentences of text around the search term in books still covered by copyright. The process is divided into two stages: Google first scans and stores the entire book in its own servers. Then, in response to a specific request by a specific user Google displays short excerpts ("snippets") of the work via its web site[31]. The Google's Library project is part of the company's general strategy to make the entire world's information available at the click of a mouse, including books and other forms of offline content.

The future and the amplitude of the Google's Library project directly depends on the application of copyright legislations, since the great majority of the contents which are digitalized and made available to the public by Google are still protected by copyright. The situation seems to be different in the U.S., Australia and Canada and in Europe, with the exclusion of U.K.

Since November 14, 2009 works included in the collections of libraries may be processed by Google's Library Project under the terms of the revised Google Book Settlement on the condition that they had been registered with the US Copyright Office by January 2009, or had been published in Australia, Canada, or the UK. An initial Settlement was reached in 2008 between Google and the Authors Guild and the Association of American Publishers pursuant to a copyright infringement lawsuit that the latter filed against the Mountain View California Company in 2005. The lawsuit was provisionally certified as a class action on behalf of all authors and publishers anywhere in the world whose works were scanned by Google. Pursuant to several objections from publishers in France and Germany, and opposition from major companies, including Amazon, the initial Settlement had to be modified in various points.

However, rival search companies are worried that having a lead role in the digitization of books could help Google to dominate another aspect of online advertising, to the possible financial detriment of its competitors[32]. Also troubling to critics is the fact that the revised settlement circumvents traditional copyright provisions by allowing Google to digitize orphan works on the basis of an opt-out model, thus without first getting rights holder permission, while any Google competitors are blocked from doing so[33]. This is a clear reversion of the classic copyright dogma that dictates that every person who wishes to exercise any right which enters in the scope of copyright protection must obtain the specific prior consent of the right holder. The solution might seem attractive from a social profit standpoint and beneficial for the public as Google does not charge for giving access to the digitalized works, but in the future the Settlement could potentially help Google to establish a de facto monopoly over the great volume of orphan works.

Apart this controversy over the possible anti-competitive effects of the Google Book Settlement, the Google Book Library Program also raises a bundle of core copyright issues, which are not the same under US and European copyright law. In the United States, the discussion focuses on whether Google's use of copyrighted works falls into the fair use defense[34] and especially whether there is a transformative one, whether the scanning of the books is an incidental copying, and whether the profit derived from advertisement revenues undermines a fair use defense[35].

In Europe, the scanning of the works necessarily prerequisites the consent of the right holders and none of the library exceptions provided by the Information Society Directive[36] could be applied to this stage. Nonetheless, the issue of displaying small segments of a copyrighted work to the specific user who made the relevant request is more controversial. Since European legislations and the Directive

2001/29/EC do not provide a general fair use defense as in US copyright law, the act of displaying of snippets to users has to be evaluated under the light of the specific copyright exceptions which are established by national copyright legislations. The question was examined by the Paris Court of First Instance. The Court ruled on December 18, 2009[37] that Google violates French copyright law, which was found applicable both to the stages of scanning of the works and of displaying the snippets[38], and firmly rejected the argument of Google that displaying a limited number of short extracts from books is covered by the exception of quotation[39]. Indeed, the Court indirectly accepted that the search of the content of digitalized books via keywords and the provision of snippets substitute the need to access the full text of the book, since they enable the users to find the information they seek[40]. Google appealed the decision.

The Google Library project adversity in France seems to be continued. On April 2010, the chief executive of major French publisher Gallimard, told AFP at Paris's annual book fair that French publishers will launch a second lawsuit against Internet giant Google for digitally scanning their books for its vast online library[41].

### *The Google "Adwords" saga*

One of the hottest IP questions that lead to a rich litigation in several EU Member States has been the involvement of Google's advertisement system "Adwords" in trademark infringement. Through "Adwords", Google allows advertisers to select keywords so that their advertisments are displayed to Internet users in response to the entry of those keywords in Google's search engine. At issue has been the legality of the use of keywords which correspond to trademarks.

French jurisprudence is particularly representative of the legal uncertainty prevailing in this area. French case law has been manifestly shown undetermined on the determination of the legal grounds of the liability of Google acting as a provider of commercial links[42]. Courts explored a variety of legal grounds either opting for the common legal regime of civil liability[43] or for the more specific grounds of trademark infringement or misleading advertising. French courts also have seemed to be divided as regards the more specific issue of trademark infringement. While at the beginning, the dominant tendency was to ascertain trademark infringement[44], more recent decisions have exonerated Google's liability due to its pure automatic and technical role in the choice of keywords or due to the application of the so-called principle of specialty[45]. According to the principle of specialty, under French law, trademark protection only extends to registration or use of identical or similar goods or services. As a corollary of this principle, trademark owners cannot prevent third parties from using their marks on dissimilar goods and services. Therefore, since Google does not provide products or services concerned by the trademark

registration, it cannot be held liable for trademark infringement. Nonetheless, this finding could lead to the following result: if the registered trademark which has been suggested by Google and used as a keyword had been registered also for advertisement services -thus services similar or identical to these provided by Google- Google's liability could be accepted[46]. Another issue, which was inextricably linked to the question of Google's liability, was the legal determination of the role of Google as a provider of a paid referencing service, and more precisely the possible application of the liability exemption for hosting providers of article 14 of Directive 2000/31/EC[47].

The jurisprudential disparity of the French lower courts lead the French Supreme Court to make three preliminary references to the European Court of Justice (ECJ) when it was called upon to settle the above issues. The facts of the three cases were quite similar. Google Adwords was found liable by French lower courts for allowing the selection of keywords corresponding to registered trade marks and for advertising Web sites offering counterfeit products or competitor sites offering similar products which did not infringe the trademarks at question.

The three references from the French "Cour de cassation" posed the following basic question: does the use by Google, in its AdWords advertising system, of keywords corresponding to trademarks constitute an infringement of those trade marks? Although the references are formulated somewhat differently, they all ask for an interpretation of Article 5(1) of Directive 89/104 and therefore concern that basic question of whether Google has committed a trademark infringement.[48] The second crucial question referred to the ECJ was whether Google could be exempted from liability on the grounds of article 14 of the E-commerce Directive[49] in case it was not held liable for trademark infringement. On March 23rd, the hotly anticipated judgments of the ECJ were published.

As regards the first question the Court concluded that while Google was acting in the course of trade, it was not using the trademarks for its own advertising service and therefore it could not be held liable for trademark infringement. More precisely, the Court found that the selection by an economic operator, by means of an agreement on paid internet referencing, of a keyword which will trigger the display of a link for the purposes of offering for sale goods or services, and which reproduces or imitates a trademark registered by a third party does not constitute in itself trademark infringement.

As regards the second question, the Court considered that article 14 of the E-commerce Directive must be interpreted as meaning that the rule laid down therein applies to an Internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider

cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned.

Hence, while Google has been clearly exonerated for liability for trademark infringement, it is still possible to be held liable on the grounds of general civil tort provisions, if it fails to comply with the obligations provided by article 14 of the E-commerce Directive. National courts will, therefore, have to evaluate the role played by Google in the course the of the creation of the advertisement and more precisely to examine whether its role is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores[50]. And the major question that has to be asked is whether Google's role is really technical. Indeed, as it is pointed out in the decision, it is apparent that, with the help of software which has developed, Google processes the data entered by advertisers and the resulting display of the advertisments is made under conditions which Google controls. In fact, Google determines the order of display according to, inter alia, the remuneration paid by the advertisers[51].

## Google Suggest and the civil tort of denigration

Google's primary function as a search engine is often accompanied by supplementary utilities whose purpose is to facilitate user's searches. This is often achieved by complementary tools based on special algorithms whose purpose is to propose to users keywords, such as the Google Adwords utility, or search terms. This is also the case of the Google suggest utility. Google Suggest is a search auto-completion tool. The utility offers search suggestions below the text which complete what the user has typed so far with a list of real time suggestions based on popular searches by other users.

One major legal question which derives from the wide use of these tools is, as it has already been remarked in the "Google Adwords" litigations, the eventual liability of Google as provider of the content which is proposed by these automated tools. The main issue is whether Google could be held liable as a content provider for infringements which might result from the content, namely the keywords or the search terms, that Google sells or proposes to its users, in spite the fact that this "content" is not generated by Google's employees but it is produced automatically by Googles' software on the basis of statistical data about the queries of Google's users. Despite the general acceptance that Google does not make choices of the eventual harmful content knowingly or on purpose, the debate is controversial because it has been proved that Google in certain occasions filters

particular kind of contents, such as pornographic content or politically sensitive content or it ranks content according to its own ranking criteria.

Indeed, despite its obvious usefulness, Google Suggest has soon become a target of serious criticism for it's mostly unfiltered suggestions, since the suggestions proposed by the tool can injure the reputation of natural or legal persons due to their insulting or depreciating content.

Two interesting and pioneer cases in France have clearly demonstrated the eventual negative implications which could emanate from the unfiltered suggestions of "Google suggest". The first case was brought before the Commercial Court of Paris in 2009. The electricity company "Direct energie" sought injunctive relief against Google for having suggested via its Google suggest utility to users the word "fraud" after they have typed into the search box the company's name. "Direct energie" argued that Google committed a civil tort through its Google's suggestion tool on the grounds of article 1382 of the French Civil Code[52], since the association of the company's name to the word "fraud", namely an illegal act, manifestly harmed its image and its reputation.

Google insisted on the automatic and statistic character of the suggestions proposed by Google suggest. It also argued that the suggestions are not illegal but obviously legitimate and useful for the whole of the community of Internet users, because they constitute the objective reflection of the researches which are statistically the most frequently carried out by the users. Nevertheless, the Court declared Google liable for having involuntarily participated to a campaign of denigration against "Direct Energie"[53]. The decision was confirmed a few months later by the Paris Court of appeals[54]. The court partially reformulated the justification of Google's infringing activity, since it estimated that the prejudice caused to "Direct Energie" derives from the lack of information about the criteria used by Google for the determination of the order of the display of the suggestions. Accordingly, the Court invites Google to transparency and orders Google to provide an explicatory notice about the way the suggestions are generated[55].

The outcome was analogous in another litigation against Google suggest in France. The facts are quite similar to the "Direct energie" case. Google was accused by the Centre National Privé de Formation a Distance (CNFDI) in a suit which claimed the search engine's 'Suggest' feature linked the organization to the word 'fraud' on the grounds of article 29 of French Law of 29th July of 1881 about freedom of press (Loi du 29 juillet 1881 sur la liberté de la presse)[56]. While the initial claim for injunctive relief filed by CNFDI resulted in a favourable ruling for Google[57], at the decision on the merits the Paris First Instance Court[58] condemned Google for denigration. In this case also the Court rejected Google's argument of lack of human involvement in the course of creation of the sugges-

tions as it found out that Google has a certain control over the content of the suggestions since it invites users to report on offensive or erroneous suggestions, and ones "that could offend", particularly "rude words and words to incite hatred or violence". A highly decisive factor that has been taken into consideration by the Court is that the CNFDI before bringing the case before the court has notified Google three times for the injurious content of the suggestions, but Google did not react.

Both cases indirectly accept that Google has been acting as a content provider or at least as a negligent host provider. The possibility of control over the content of the suggestions eradicates Google's argument about the automatic character of the suggestions. This element has also been proven to be critical for the acceptance of Google's involuntary participation to the denigration of the claimant in the first case and of Google' intention to harm the claimant in the second case. Despite the evasive justification of the Courts on this issue, it can be deducted that the generation of the suggestions on the basis of popular search queries via an automatic process does not preclude the existence of a fault and more precisely Google's willful or negligent participation to the denigration. The cases also reaffirm the classic rule of media law that a person may be held liable for defamation and injury to reputation even if she simply repeats the offensive content which has been originally created or published by another person[59].

## Google's ranking tactics and European competition law

"Googling" has become an autonomous concept and an independent form of leisure activity, similar to "zapping" through television channels. Anybody who cannot be found via Google does not exist: To exist is to be indexed by a search[60.] This is highly important for every person or entity who has a presence in the World Wide Web, but even more crucial for other search engines which compete Google in the information market.

Google's ranking tactics concerning its competitors have been officially contested by three European Internet companies before the European antitrust authorities. The inquiry, disclosed on February 2010, appears to focus largely on complaints that Google unfairly ranks the sites of the Internet competitors, in effect lowering their rank in search results that appear on Google sites. In that way it penalizes potential competitors and keeps advertising prices artificially high[61]. Moreover, Google has been accused for abusing its dominant position in the market of search engines in order to promote its own service. Especially, Shivaun Raff, the chief executive of one of the companies which filed the complaints, the UK company Foundem, told BBC Radio 4's *Today* program, in the last couple of years Google has started to use its search results as a marketing channel for its own

services: "When a user typed in a query about a specific item they wished to buy or research, she said, "you would find near the top 'shopping results' and that is Google's own price comparison service inserted. And you will also see 'video results', and that is Google's own video service"[62].

The legal ground of the claims is the abuse of Google's dominant position in order to demote the Web sites of Google's competitors. The complaints against Google come at a time of scrutiny of Google in Europe, where the company has an even more dominant position in search advertising than it does in the U.S. As the case is still at an early, fact-finding stage and there is not any official information about the legal arguments and the exact content of the complaints, an analysis of these cases is not possible. However, it is very interesting to follow closely these cases, since apart from privacy law, intellectual property law and tort law Google's legal adventures seem to extend also in the field of European competition law.

Except for the eventual anticompetitive activities of Google concerning the exclusion or depreciation of its competitors for the profit of its own services, the ranking of businesses upon a payment and the sale of keywords could also raise significant competition issues for third parties which use Google's services. Indeed, the appropriation of keywords by certain companies on several major search engines, such as Google that dominates the market of search engines in Europe, could possibly prevent the companies of the same sector to be visible on Internet and, as a result, to almost completely exclude them from this market[63]. This interesting hypothesis has been examined by the French Competition Authority in 2000[64]. At this time, the Competition Authority concluded that competition law rules could not justify any obligation of the search engines to index and rank information in an exhaustive or objective way. Nevertheless, it was not excluded that, according to the context, an agreement between a search engine and a commercial Website for a priority or exclusive referencing via the reservation of keywords could be considered as anti-competitive.

## Conclusion

Google is one of the most characteristic examples of how a private company can force law to advance and explore its limits. Indeed, Google's leading activities in various information technology sectors have undoubtedly been the source of new legal challenges. European information law had to deal with multiple legal issues in the fields of data protection law, intellectual property law, tort law and recently competition law. In the majority of cases, European jurisdictions applied firmly the European legal principles and EU legislation and obliged Google to reconsider its business strategy at least in Europe. Nonetheless, Google's vari-

ous European litigations have created a rich case law that constitutes by itself a significant evolution of European information law. Since Google continues to expand its activities constantly, the emergence of new legal questions is just a matter of time.

## Endnotes

1. For a quasi-exhaustive description of Google's products and services, see: http://www.webrankinfo.com/google/produits.php.
2. Sherman, Chris. Google power: unleash the full potential of Google. p. 415, http://books.google.com/books?id=SRadJIuhVjAC&dq=Google+Power;+Unleash+the+Full+Potential+of+Google&q=Daniel+Brandt#v=snippet&q=Daniel%20Brandt&f=false.
3. Article 29 of the Data Protection EU Directive 95/46 (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) establishes a "Working Party on the Protection of Individuals with regard to the processing of Personal Data". It is generally known as the "Article 29 Working Party". It is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the EU Commission.
4. Letter addressed to Google Inc., dated May, 16th 2007, D (2007) 6016.
5. Opinion on Search engines (WP148, 4 April 2008). See also: International Working Group on Data Protection in Telecommunications, Common Position on Privacy protection and search engines on 15 April 1998, revised on 6-7 April 2006 (http://www.datenschutz-berlin.de/doc/int/iwgdpt/search_engines_en.pdf)· 28th International Data Protection and Privacy Commissioners' Conference, Resolution on Privacy Protection and Search Engines, London, 2 – 3 November, 2006 http://www.privacyconference2006.co.uk/index.asp?PageID=3).
6. Search engine providers do not act as simple intermediaries in case they perform value-added operations linked to characteristics or types of personal data on the information they process. In such cases the search engine provider is fully responsible under data protection laws for the resulting content related to the processing of personal data. The same responsibility applies to a search engine that sells advertisement triggered by personal data – such as the name of a person. Search engine providers do not act as simple intermediaries also as regards their caching functionality and any caching period of personal data contained in indexed websites beyond this necessity of technical availability of the website, should be considered an independent republication. See: Opinion on Search engines (WP148, 4 April 2008), op. cit., p. 14-15.
7. See article 7 (f) of the Data Protection Directive.
8. See pages 17-18 of the Opinion 1/2008, op. cit.
9. 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.
10. 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, OJ L 105, 13.4.2006, p. 54–63.

11. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108/33, 24.4.2002.
12. Opinion 1/2008, op. cit., p. 12.
13. Maggie Shiels, Google Buzz 'breaks privacy laws' says watchdog, http://news.bbc.co.uk/2/hi/8519314.stm.
14. See: Google Blog "Another step to protect user privacy" (8 September 2008), URL: http://googleblog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html.
15. A. Frome/G. Cheung/A. Abdulkader/M. Zennaro/B. Wu/A. Bissacco/H. Adam/H. Neven/L. Vincent, Large-scale Privacy Protection in Google Street View. Available on line at: http://static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/el//archive/papers/cbprivacy_iccv09.pdf.
16. Article 29 Data Protection Working Party, Press release, Brussels, December 10, 2008. Available on line at: http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_10_12_08_en.pdf.
17. See "TN/ΕΞ/374/14-04-2009" document of the Greek Data Protection Authority. Recently the Greek Data Protection Authority issued a decision about the processing of personal data by the service "kapou.gr" whose function is identical to the Google street view service (Decision 91/2009). In this decision, the Data Protection Authority makes an express reference to its former Google street view decision and states that the same measures should be adopted for both services. The decision examines thoroughly all the stages of data processing by panoramic street-level view services. After having evaluated all the privacy protection measures taken by the service "kapou.gr" under to its prior recommendations, the Data Authority authorizes the service to operate in Greece.
18. Indeed, privacy infringement due to the processing of images of houses instead of persons is more difficult to establish because the picture of a person's residence is a form of indirect identification which has to be combined with other elements, such as the address, in order to reveal the person's identity. In the USA, the District Court of Pennsylvania dismissed the claim of a couple that sued Google over an alleged privacy violation (more specifically invasion of privacy, trespass, injunctive relief, negligence, and conversion) after a Street View image of their property was posted to the web. The couple sought compensatory, incidental, and consequential damages in excess of $25,000 for each claim, plus punitive damages. On February 17, 2009, the District Court granted Google's motion to dismiss as to all of the couple's claims. The Court dismissed the invasion of privacy claim because the claimants were unable to show that Google's conduct was highly offensive to a person of ordinary sensibilities. See Boring v. Google, Inc., 598 F. Supp. 2d 695, 699-700 (W.D. Pa.2009). On January 25, 2010, the U.S. Court of appeals (3rd circ., no 09-2350) affirmed the District Court's grant of Google's motion to dismiss the Borings' claims for invasion of privacy, unjust enrichment, injunctive relief, and punitive damages, but reversed with respect to the trespass claim and remanded with instructions that the District Court permit that claim to go forward. See: http://www.ca3.uscourts.gov/opinarch/092350np.pdf.

19. See http://en.wikipedia.org/wiki/Criticism_of_Google. Google equipped its vehicles with antenna as well as cameras so it could create a database with the names of Wi-Fi networks and the coding of Wi-Fi routers. However, some experimental software was being used in the Street View project, and that programming picked up the Web surfing on publicly accessible Wi-Fi networks if the company's vehicles were within range of the signal. However, Google only gathered small bits of information because its vehicles were on the move and its tracking equipment switched channels five times a second. See: http://www.pe.com/business/local/stories/PE_Biz_D_google15.40fde5c.html.
20. http://en.wikipedia.org/wiki/Google_News.
21. There are billions of Web pages accessible on the Internet. It would be impossible for Google to locate and index or catalog them manually. Accordingly, Google, like other search engines, uses an automated program (called the "Googlebot") to continuously crawl across the Internet, to locate and analyze available Web pages, and to catalog those Web pages into Google's searchable Web index. As part of this process, Google makes and analyzes a copy of each Web page that it finds, and stores the HTML code from those pages in a temporary repository called a cache. Once Google indexes and stores a Web page in the cache, it can include that page, as appropriate, in the search results it displays to users in response to their queries. When clicked, the "Cached" link directs an Internet user to the archival copy of a Web page stored in Google's system cache, rather than to the original Web site for that page. By clicking on the "Cached" link for a page, a user can view the "snapshot" of that page, as it appeared the last time the site was visited and analyzed by the Googlebot. For this description, see: Field v. Google Inc., No. CV-S-04-0412-RCJ-LRL, United States District Court District of Nevada (2006).
22. The quasi-proprietary database *sui generis* right is established by the Directive 96/9/EC: 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.
23. Ph. Laurent, Case Note, Google News banned by Brussels High Court – *Copiepresse SCRL v. Google Inc.* – Prohibitory injunction of the President of the High Court of Brussels, 5 September 2006, Computer Law & Security Report 23, 2007, p. 84.
24. Ph. Laurent, op. cit., p. 83. However, as the author remarks, it is noticeable that in the USA the District Court in Nevada has recently ruled that serving a webpage from Google cache does not constitute direct infringement and is, in any case, fair use. See: *Field v. Google Inc.*, No. CV-S-04-0412-RCJ-LRL, United States District Court District of Nevada (2006).
25. TPI Bruxelles, 5 septembre 2006. Available on line at: http://www.droit-technologie.org. Also see: Van den Bulck P./Wery E./Bellefroid M., Google News sur la sellette, Le triomphe de David sur Goliath?, http://www.droit-technologie.org.
26. TPI Bruxelles, 13 février 2007. See: Van den Bulck P., Copiepresse contre Google: les limites du «caching»? Revue Lamy Droit de l'Immatériel, avril 2007, 67.
27. See: http://www.kluweripcases.com/. For the US see the See: Field v. Google Inc. case, op. cit.
28. These fall within the perimeter of art. 31 I of the Ley de Propiedad Intelectual.
29. For the interpretation of the three-step test, see Lucas A./Lucas H.J., "Traité de la propriété littéraire et artistique", 3e édition ; Lexis Nexis, Litec, 2006, p. 269· M. Senftleben, Copyright, Limitations and the Three-Step Test - An Analysis of the Three-Step Test in Interna-

tional and EC Copyright Law, Kluwer Law International, The Hague 2004· Ginsburg, J. C. (2001), "Toward Supranational Copyright Law? The WTO Panel Decision and the "Three-Step Test" for Copyright Exceptions", Working Paper No. 181 of the Columbia Law School - For Revue Internationale du Droit d'Auteur, pp. 1- 16· M. Ficsor, "How much of what? The three-step test and its application in two recent WTO dispute settlement cases", RIDA 2002, n°192, p. 145· also M. Ficsor, "EBU Copyright Symposium, Quo vadis, Copyright", Barcelona, March 31, 2006, "How did we arrive here? The evolution of copyright legislation , www.ebu.ch, p. 6· Chr. Geiger, "The role of the three-step-test in the adaptation of copyright law to the information society" e-Copyright bulletin, January-March 2007. Available on line at: http://portal.unesco.org/culture/en/files/34481/11883823381test_trois_etapes_en.pdf/test_trois_etapes_en.pdf· Gervais, D. (2005), "Towards a New Core International Copyright Norm: The Reverse Three-Step Test", Marquette Intellectual Property Law Review, vol. 9, no. 1, p. 1· Gautier P.Y., "L'élargissement des exceptions aux droits exclusifs, contrebalancés par le «test des trois étapes», Communication-Commerce Électronique, novembre 2006, p.11· T. Sinodinou, Voyages des sources du test des trois étapes aux sources du droit d'auteur, Revue Lamy Droit de l'immatériel, août/septembre 2007, p. 74. Also see Declaration, A balanced interpretation of the three-step test in copyright law, p. 4. Available on line at: http://www.ip-institute.org.uk/pdfs/Jonathan_Griffiths_Declaration.pdf, IIC (39) 2008, p.707· Huaiwen H., Seeking a Balanced Interpretation of the Three-Step Test - An Adjusted Structure in View of Divergent Approaches, IIC (40) 2009, p. 274.

30. Raquel Xalabarder, Case summary and Annotation of the September 17th, 2008 decision of the Provincial Court Barcelona (Audiencia Provincial Barcelona), http://www.kluweripcases.com/.

31. Band Joseph (2006). The Google Library Project: Both Sides of the Story. Plagiary: Cross-Disciplinary Studies in Plagiarism, Fabrication, and Falsification, 1 (2): 1-17. See also Bottis M., The google Library Project, TEKMIRION 2007,7, pp. 175-188, (in Greek).

32. Chris Lefkow (AFP), Last-minute objections filed to Google book settlement, January 28, 2010, http://www.google.com/hostednews/afp/article/ALeqM5gi8ydpiQlS04Qe_zy6vnmdCrQkMQ.

33. http://news.cnet.com/8301-1023_3-10398995-93.html.

34. According to section 107 of the title 17 of the US Copyright Code, "Notwithstanding the provisions of sections 106 and 106A, 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. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors".

35. Agnes-Lucas Schloetter, Digital libraries and copyright issues Digitization of contents and the economic rights of the authors, in: Iglezakis/Kapidakis/Synodinou, «E-Publishing and Digital Libraries: Legal and Organizational Issues», IGI Global, 2010 (under publication).

36. 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, OJ L 167, 22.6.2001, p. 10.
37. Tribunal de grande Instance de Paris, December 18, 2009. Available on line at: http://juriscom.net/documents/tgiparis20091218.pdf.
38. The determination of private international law was one of the more delicate issues of the case. Google argued that U.S. copyright law had to be applied on the grounds of article 5 par. 2 of the Berne Convention, since the infringing acts or reproduction and representation took place in the U.S. For an analysis of these points, see: F.M. Piriou, La numérisation des livres sans autorisation constitue un délit de contrefaçon, Communication-Commerce Electronique, mai 2010, p.16. U.S. copyright law was found applicable in another copyright case against Google in France, the so - called "Google Images" case where Google was relaxed thanks to the application of U.S. law. See TGI Paris, 3e ch., sect. B, 20 mai 2010, SAIF c/ Google France, Jurisdata n° 2008-362899, Communication-Commerce Electronique, 2008, Etude 22, Y. Gaubiac.
39. As Lucas-Schloetter points out, since Google does not really make copyrighted works available, but only searchable, it may therefore be argued that the limited amount of the copyrighted work made accessible to the users of Google's search engine is the key issue in assessing the lawfulness of Google Book Search Library Program under European copyright legislation. Nonetheless, the French exception for quotation is considered as narrow, since it only allows the making of analysis and short quotations justified by the critical, polemical, educational, scientific or information character of the work into which they are incorporated (art. L. 122-5 3° (a) of the French CPI). See Agnes-Lucas Schloetter, Digital libraries and copyright issues Digitization of contents and the economic rights of the authors, op. cit. The exception for quotation which is provided by the Directive 2001/29 is wider as it does not set a strict limit concerning the extent of the quotation and does not presuppose that the quotation has to be incorporated in another work. However, it requires that the quotation must be in accordance with fair practice and it must be done for a specific purpose. See Bechtold, in Dreier/Hugenholtz, Concise European Copyright Law, Kluwer Law International, 2006, p. 379.
40. F.M. Piriou, La numérisation des livres sans autorisation constitue un délit de contrefaçon, op. cit., p. 17.
41. See http://www.smh.com.au/technology/technology-news/google-faces-new-bookscanning-lawsuit-20100401-rg0b.html.
42. Féral-Schuhl Chr., Fournisseurs de liens commerciaux, une jurisprudence encore indécise..., Revue Lamy Droit de l'Immatériel, n°36, mars 2008, p. 47.
43. See for example Trib.com. Paris, 15e ch., 24 novembre 2006, sté One tel c./ Stés Google et Olfo, RLDI 2007/24, n°776. For a commentary of this case, see: Tardieu-Guigues E., Liens commerciaux: condamnation de Google en dehors du droit des marques, RLDI, mars 2007, n°25, p. 9.
44. CA Versailles, 23 mars 2006, Sté Google France c./Sté CNRRH et autre, n°05/00342, RLDI 2006/16, n°470, obs. Costes· TGI Nanterre, 2e Ch., 14 décembre 2004, CNRRH, Pierre Alexis T c./Google France et a., Propriétés Industrielles, 2005, n°4, p. 23-24· TGI Nanterre, 2 mars 2006, Hôtels Méridien c./Google France. Available on line at: http://www.legalis.

net· CA Paris, 4e ch., sect.A, 28 juin 2006, Google France c./Louis Vuitton Malletier. Available on line at: http://www.legalis.net.

45. TGI Paris, 8 decembre 2005, Kertel c./Google. Available on line at: http://www.legalis.net· TGI Paris, 12 juillet 2006, Gifaml c./Google, RLDI 2006/20, n°605· TGI Nice, 7 février 2006, TVD Industries c./Google. Available on line at: http://www.legalis.net· TGI Paris, ord., 11 octobre 2006, Citadines c./Google. Available on line at: http://www.legalis.net· TGI Paris, 13 février 2007, Laurent c./Google. Available on line at http://www.legalis.net· TGI Strasbourg, 20 juillet 2007, RLDI 2007/30, n°966. Google was also found not liable for trademark infringement in Germany: Landgericht Munich, 12 dec. 2003, Az. 33 0 21461/03, X v. Google, voy. See F. Hofer, Legal problems of search engine marketing, April 2004, p. 10, available on line at: http://www.hltlaw.it.
46. Glaize F., Liens publicitaires: suggérer est-ce contrefaire?, RLDI, mars 2008, n°36, p.53.
47. 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 P. 0001 – 0016. According to this article 14 par. 1 of the e-Commerce Directive "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".
48. According to this provision, "The registered trade mark shall confer on the proprietor exclusive rights therein. The proprietor shall be entitled to prevent all third parties not having his consent from using in the course of trade: (a) any sign which is identical with the trade mark in relation to goods or services which are identical with those for which the trade mark is registered; (b) any sign where, because of its identity with, or similarity to, the trade mark and the identity or similarity of the goods or services covered by the trade mark and the sign, there exists a likelihood of confusion on the part of the public, which includes the likelihood of association between the sign and the trade mark". The concept of in the "course of trade" has been interpreted broadly by the ECJ in the Arsenal/Reed Case (C-206/01), 12 November 2002, *Arsenal Football Club v. Matthew Reed:* "In those circumstances, as the national court stated, the use of the sign identical to the mark is indeed use in the course of trade, since it takes place in the context of commercial activity with a view to economic advantage and not as a private matter" (point 40 of the decision).
49. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services.
50. See point 114 of the decision.
51. See point 115 of the decision. See also: L. Thoumyre, Impact de l'arrêt Google Adwords de la CJUE sur la responsabilité des services 2.0. Available on line at: http://.www.juriscom.net· L. Grynbaum, Google Adwords: l' hébergeur, un prestataire nécessairement passif, Revue Lamy Droit de l'immatériel, mai 2010, p. 38.

52. "Direct energie" founded its claim on articles 1382 of the French Civil Code and 873 of the French Code of Civil Procedure. According to article 1382 of the French Civil Code any act whatever of man, which causes damage to another, obliges the one by whose fault it occurred to compensate it.
53. Tribunal de commerce de Paris Ordonnance de référé 7 mai 2009, Direct Energie / Google Inc. Available on line at: http://www.legalis.net.
54. Cour d'appel de Paris Pôle 1, 2ème chambre Arrêt du 9 décembre 2009, Google Inc/Direct Energie. Available on line at: http://www.legalis.net.
55. See: A. Debet, comment on Cour d'appel de Paris Pôle 1, 2ème chambre Arrêt du 9 décembre 2009, Google Inc/ Direct Energie, Communication-Commerce Electronique, mai 2010, p. 31.
56. According to this article, "Toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait est une injure ".
57. TGI Paris, réf., 10 juillet 2009, n°9/55969, Centre National Privé de Formation à Distance (CNFDI) c/Sté Google Inc. Available on line at: http://www.legalis.net.
58. Tribunal de grande instance de Paris, 17ème chambre, Jugement du 4 décembre 2009, JPL-CNFDI/Google Inc. Available on line at: http://www.legalis.net/.
59. A. Cousin, «Google Suggestions»: injure sans intention de nuire ou dénigrement involontaire?, Revue Lamy Droit de l'immatériel, aout/septembre 2009, p. 28.
60. Nico van Eijk, Search Engines: Seek and Ye Shall Find? The Position of Search Engines in Law, IRIS, Strasbourg January 2006, p. 2.
61. http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article7038845.ece.
62. http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article7038845.ece?token=null&offset=0&page=1.
63. S. Pirlot de Corbion, La responsabilité des fournisseurs d' outils de recherche sur Internet, DA/OR, 2004/72, p. 29. Available on line at: http://www.droit-technologie.org.
64. Conseil français de la concurrence, décision no 00-D-32 du 9 juin 2000 relative a une saisine au fond et une demande de mesures conservatoires présentées par la société Concurrence. Available on line at: http://www.conseilconcurrence.fr.

# Open access repositories and freedom of information

**Roxana Theodorou**

For the last two decades at least, academic (and not only academic) libraries are facing serious economic problems that do not allow them to serve their purpose to the fullest. Additionally, subscriptions to scientific journals have been rising to extraordinary levels, making the situation even more difficult. In fact, between 1975 -1995 the prices of subscription based journals have risen to 300% above inflation (Tenopir and King, 1997). After 1995 and until today, subscriptions continue to rise rapidly, although, to be fair, not as much as previously. It is, however clear, that library budgets cannot meet these financial demands. So, libraries try to face their problems, mainly by forming consortia that negotiate prices with publishers and try hard to address the needs of their users as best as they can.

But how did the publishing world became so tough? Until WW2 academic publishing was mainly in the hands of universities and learning societies (Cox, 2005). With the end of WW2, there was an ever-rising interest in science and scientific information. Commercial publishers saw an opportunity there and were very keen and quick to invest, buying out small publishers or simply founding new journals. Through time and after many mergers and acquisitions, today, scientific publishing is in the hands of a few, very important and very fierce publishers. And because of this new found oligopoly they have the power to decide and enforce the rules of the game.

Additionally, academic publishing belongs to a special kind of market; it's a two-sided market (Rochet & Tirole, 2005, Roson, 2005). Two-sided markets, also called two-sided networks, are economic networks having two distinct user groups that provide each other with network benefits. Example markets include credit cards, composed of cardholders and merchants; HMOs (patients and doctors); operating systems (end-users and developers), travel reservation services (travelers and airlines); yellow pages (advertisers and consumers); video games (gamers and game developers); and communication networks, such as the Internet. Benefits to each group exhibit demand economies of scale. Consumers, for example, prefer credit cards honored by more merchants, while merchants prefer cards carried by more consumers. In two-sided markets the act of creating a good and giving it to consumers cannot be separated. That, in fact, means that the intermediate has an additional power in deciding the price of the product.

Another paradox about academic publishing is that the end user (namely the reader) is rarely ever burdened with the cost of the product. Libraries are those that have to pay for scientific journals and ensure that the users will have continuous and unhindered access.

Also, the authors of scientific content almost in whole belong to the institutions that buy their works in the form of published articles. But the fact is that part of the authors' salaries is for that purpose exactly: to research, write and publish their conclusions. So the institution ends up paying twice for the same product, which partly belonged to them in the first place.

In order for libraries to cope with the increasing prices of subscriptions, they have formed coalitions that negotiate with the publishers in order to ensure lower rates and better terms of access. And although, at first there was some success, the prices are still too high, and with the help of secret deals with some of the partners of coalitions publishers have managed to prevail, once again.

Open access is a very popular term nowadays. There are many implementations of open access with the two most important being open access journals and open access repositories. Each implementation has its own advantages and disadvantages that academic libraries and institutions can examine and try and find the most efficient way to publish scientific information.

The goal is always to create a product that is cheap (or at least cheaper), easy to use, reliable and of high quality. Using the experience of the past and combining partnerships through coalitions and open access implementations, we now propose a new publishing system that could take libraries and institutions out of their very difficult situation.

The business model of coalition publishing is based on the idea of "returning" the dissemination and administration of scientific publishing to the hands of academic institutions and their corresponding libraries. The basic idea is this; institutions of the same scientific interest form publishing coalitions and create and maintain cross institutional repositories in which they publish (in electronic form only) all the scientific production of their members (and anyone else interested, as long as the works cover the given subject). But, in order for these repositories to be able to compete against subscription based journals their contents should be of high quality. That means that they should undergo some kind of selection policy, the best till now being, peer review.

Half of the existing open access repositories are subject based. And only 13% of those are cross institutional (OpenDOAR, 2010). But, till now, there are no certain selection policies enforced that ensure the quality of the contents. And there is no certain way to tell either, what *kind* of works are accumulated in them (the-

ses, articles, preprints or post prints, teaching material etc). It would then be fair to say that till now, the contents of institutional repositories are not considered equally useful and credible as that of scientific journals.

Most academic and scientific libraries in their effort to develop and offer e-services to their users come to face a phenomenon known as competitive convergence. This actually means that competitive establishments, in their effort to obtain competitive advantage, come to use the same techniques and offer the same services in a similar way. The only way to break this vicious cycle is for a business to try and find the functions that make it unique in its market and try and use them to its benefit. In the case of academic libraries that could mean that they have to manipulate and use some the practices of their competitors.

A subject-based repository has a starting advantage. Its content is fairly obvious. The user can automatically know which science is covered in any particular repository and not lose time and effort looking among information irrelevant to her research. But of course, thematic relevance is not enough. In order for a repository to be really of use to its users has to be exhaustive, inclusive, valid, and up to date. These characteristics can only be achieved through the active participation of as many authors as possible. But authors also need some incentives in order to submit their works in a repository, instead of an established scientific journal. The repositories should provide that:

- In the coalition take part scientific/research and teaching institutions acclaimed internationally at their respective fields. This will draw to the coalition smaller institutions which wouldn't otherwise attempt such an ambitious project. It will also give the guaranty needed to the authors for the credibility and longevity of the repository.
- The repository should include as many file formats and genres of works as possible. On the same time though there must be a strict selection policy enforced, that will clearly state what should and should not to be included in the repository. This two should be carefully balanced so that they do not to mutually cancel one another.

Much like traditional library coalitions, cooperative subject repositories have to be centrally controlled in order to function properly. But on the same time, the goal has to be the creation of a flexible and effective cooperative union in order to survive in the world of scientific publishing.

Probably the most effective way to go about it would be to create a central management system that would encompass the basic logic of a P2P network. That way all of the participants will have equal access to and share resources, control

and responsibility of procedures. P2P networks can be separated into 3 different categories.

1. Centralized (1st generation) networks. There is a centralized index server on which is stored information about the contents of the files that the users wish to share. Users search the index server and when the desired document is fount a link opens between the user and the owner of the file. (Napster and DC++ are examples of such networks)
2. Decentralized (2nd generation) networks. The philosophy here is completely different. Every system that participates in the network serves both as client and as server. As long as someone is connected to the network with the use of the appropriate software his existence is made known to a small group of connected computers, which in turn, make their existence known to a larger group of computers etc. The user can, this way, search for any information on the shared files between the connected computers.
3. 3rd generation. These networks have mainly characteristics of anonymity, like Freenet and Entropy. They are decentralized, and their philosophy is based, besides anonymity, on high viability, constant file sharing, and encoding, so that no one ever can take absolute charge of the network. This kind of networks is still evolving and has been characterized as small global networks.

Creating small and closed off repositories will not contribute much to scientific information. One main reason why repositories exit is that they function as a vivid, living, growing advertisement of the institution they belong to and an easy way to manage their scientific production. But a repository could not be only that, otherwise it is damned to wither and die.

It would be difficult to describe in such a short time the whole organization of the proposed model. But, in rough terms the concept is this:

1. Following the necessary negations institutions of the same orientation agree to form a publishing coalition. In order to maintain the cost low, publication should be only in electronic form.
2. The definitive structure of the coalition will not be discussed at this presentation but it would certainly have a basic managerial department that organizes the whole business, and two basic departments one for administrative and another for economic affairs.
3. The most difficult part of this project would be, of course, the funding. Funds could come from a variety of places:

a. Advertisements, if the coalition desires it, there could be some advertisement space on the site of the repository that could in fact generate a steady income.

b. Author payments. Authors pay a small fee in order to publish their works. Of course in order for author to be *willing* to pay, the repository should ensure that the quality of its services is very high.

c. Member fees. All members of the coalition pay annual fees in order to sustain the repository. The fees depend on the size of each institution.

d. Added value products. Although the publications of the coalition are strictly in electronic form, in order to lower costs, if a user wishes to obtain a printed and bind volume of, let's say, a collection of works, this service could be charged extra. Almost all institutions have a publications office that is already equipped to do such works, so it wouldn't be really difficult to organize such services.

e. Public funds. Most scientific institutions are already funded (partly or in whole) by the governments of their countries. A small part of these funds could be reallocated to cover some of the expenses of the publishing coalition. If the project meets success, then the coalition could ask for additional funds (taking into account that subscriptions to scientific journal will be a lot less).

f. Private funds. The coalition could ask for donations from private donors.

4. Depending on the structure of the coalition, it should be decided where and how the servers and the services are based.

5. Finally, we have the organization of the peer review process. In the case of cooperative subject repositories peer review can be enforced in two distinct stages, before and after publication, intensifying the participatory process and upgrading the role of the reader to reviewer. More precisely, at first, groups of 2 or 3 reviewers (that come from the institutions that take part in the coalition) assess in a blind process the submitted works and decide whether it gets published or not, if there is any need for editing etc. After publication the review process is open to the public and the readers can place their comments on the site (of course the moderator of the site, always, retains the right to delete any comments that are insulting, irrelevant or in any way inappropriate). The process of open review can quickly transform itself into a need kind of citation method, especially if the users start to interlink relevant works and comments to the original work, making this way, new research more visible and creating a more intense impact for any published work.

But, what comes to everybody's mind when we talk about publishing (or any other kind of business for that matter) is how much does it cost? Publishing in a repository, even if we take into account peer review, is very much cost effective.

The cost can be broken down into many categories. There is the cost of the installation of the software, the cost of any customization needed, salaries for the staff, functional costs etc.

According to S. Gibbons (2005), installation and maintenance cost of a repository can vary dramatically, depending on its size and orientation. It depends on the software chosen (whether it is open source or commercial), the number of people working for the repository, the equipment that will be used etc. If the institution chooses to join SHERPA then the cost of mere installation (the cost of the server and man-hours) comes up to €4.300. Queen's University, QSpace, cost for the organization and setting up, €37.000 (including, equipment, customization and salaries). It also costs €37.000 / p.a. to maintain the repository.

Presumably, the repository with the largest setting up and maintenance cost in that of MIT, which is considered the most advanced and complicated of its kind. Setting up MIT's DSpace cost €1.307.000, but we should take into account that this figure includes the cost of the development of DSpace, an open source software used globally by a large number of users and institutions. The annual maintenance cost of the repository is a lot less, of course, and it totals €207.000. This includes all the costs of the repository (hardware, software, functional costs) and all the salaries and insurance costs of the staff.

The repository of the University of Rochester cost around €145.000 to set up, with major customizations. At this point, the repository has more than 50 collections depending on the subject and the department they serve.

Houghton, on his JISC repost on 2009 determined the total cost of an article from the time the author captures the concept until it gets processed from a library and is finally available to the users. Houghton calculated this cost to be €10.600. From that figure only a small part burdens the publisher. And depending the form of publication the publishing cost may vary. In the case of subscription based journals the publishing cost is €2.580 (for e-only publishing), and for open access journals the publishing cost is €1.682. In the case of open access repositories (and if a paper is submitted for publication only once) the publishing cost is even lower, although it very hard to determine exactly.

But what can be determined is the cost per article for the system of higher education depending on the form of publication. For subscription based journals the cost for HE is €9.160 / per article, for open access journals is €8.262 and for OA repositories €8.262. It should be noted that this figure includes the peer review

process. The cost differences are very big and should be taken seriously into account.

But a project as ambitious as this could face a number of problems:

1. there could be difficulties for different institutions to reach agreements
2. There could be lack of funds for the initial stages of the project.
3. Members of the coalition may disagree in the use of standards and procedures.
4. The larger and more robust members of the coalition may try to enforce their priorities to the other members.
5. If there is no robust business plan and clear priorities the project could reduce itself in mere vision.
6. Commercial publishers will oppose to such an effort and try to boycott it in any way possible.
7. Lack of cross-functionality between different applications.

But there is also some true potential to such a project:

A cross institutional repository is economically viable and cost effective. It is not just easy to maintain but also, if it functions properly and grows in time, it could save serious money from cancelled subscriptions.

Researchers themselves seem to be every day more eager to participate in open access mediums. Open access journals are growing and repositories are being constantly set up in all kinds of institutions. On January 2008 there was an unprecedented movement of support of Open Access. The European research council and the US National Institute of Health officially adopted their open access mandates. But that was not the end of it. 8 other very important organizations actively supported open access. Of course, these movements are not the only ones. All around the world, publicly funded research bodies are supporting open access, either by setting up repositories, either by encouraging researchers to submit their works in open access mediums or by adopting open access mandates.

The advantages of OA are many, especially when high standards of quality are achieved. Access to scientific results becomes easier and quicker. This saves time and money not only to researchers themselves, but also for their funding bodies, institutions and libraries. On the other hand, open access articles are more likely to be cited compared to the subscription based model. This means increased visibility for the work and the authors and their institutions.

Maybe it is still too early to come to any definite conclusion as to how open access is going to be in the future. But for the time being it seems that repositories

will play an important part in scientific communication. Open access is not going to be the only publishing alternative in the near future. But its popularity can be a force for changes. Coalition publishing cannot completely overturn the present status quo, which exists and serves scientists and scientific information for nearly 350 years. But, it can, and probably will be, the excuse and means needed in order to improve the system to the benefit of society.

## References

Tenopir C., King D. W., 1997, Trends in scientific scholarly journal publishing in the U. S., J. Scholarly Publishing, 48 (3), 135-170

Rochet, J.-C. and J. Tirole, 2004, Two-Sided Markets; An Overview, Mimeo IDEI, Toulouse. [online] Available at: http://faculty.haas.berkeley.edu/HERMALIN/rochet_tirole.pdf

OpenDOAR, Directory of Open Access Repositories, http://www.opendoar.org/

Houghton, J., 2002, The Crisis in Scholarly Communication: An Economic Analysis, Paper presented at the meeting of the Victoria Association for Library Automation 2002.

Jefferson, T., P. Alderson, E. Wager, and F. Davidoff, 2002a, Effects of editorial peer review: A systematic review. Journal of the American Medical Association 287:2784–2786

King, D.W., 2007, The cost of journal publishing: a literature review and commentary, Learned Publishing 20(2), April 2007, pp85-106.

McCabe, M. J., 2004, Information Goods and Endogenous Pricing Strategies: the Case of Academic Journals, Economics Bulletin, 12(10), 1-11.

Odlyzko, A., 1998, The economics of electronic publishing, Journal of Electronic Publishing, 4(1). [online] Available at: Http://quod.lib.umich.edu/cgi/t/text/textidx?c=jep;view=text;rgn=main;idno=3336451.0004.106.

Gibbons, S. (2004). Establishing an Institutional Repository. Library Technology Report. 40:4, pp. 11-14.

Gibbons, S. (2005). Establishing an Institutional Repository. LITA Regional Institute. November 8, 2005, Available at: http://docushare.lib.rochester.edu/docushare/dsweb/Get/Document-19852/Establishing%20an%20Institutional%20Repository.ppt

Houghton, J.W. & Oppenheim, C. (2009) The Economic Implications of Alternative Publishing Models. Prometheus 26(1): 41-54 http://www.informaworld.com/smpp/content~db=all~content=a920247424

# The right in confidentiality and integrity of information technology systems according to the German federal constitutional Court: old wine in new bottles?

**Stavros Togias**

## Introduction

A wide range of criminal activity–encompassing among others organized crime, right or left-wing extremists and Islamic terrorist groups–uses information technology not only for the accomplishment of its propaganda objectives, but also to ensure a principally secret communication, ideal for the preparation and execution of criminal plans. On the other hand, law enforcement agencies are standing on the threshold of a new era, facing the risk of being pushed out of the limelight of crime detection, due to the rapid progress of information technology and the prevailing patterns of conspiration and detection-proofing of criminal networks [Livos, 2007].

Thus, the traditional and routine investigative measures, such as interception of telecommunications, tend to become pointless as modern offenders either refrain from transmitting crime-related information over the telephone or the Internet, or, in the rare case when they do so, they employ elaborated encryption technologies [Hofmann, 2005].

In contrast, the novel online search [online Durchsuchung] seems to promise successful investigation of such serious crimes and, likewise, to counteract the aforementioned demerits of outdated investigative techniques. The online search facilitates the covert electronic intrusion into the storage media (e.g. hard drive) of the targeted computer unbeknownst to its user. This controversial investigative technique appears particularly beneficial with reference to criminal organisations, since it both enables the prompt collection of electronic data –i.e. at the preparatory stages of the commission of a felony and before the encryption of the crime-related information [Federrath, 2009]– and does not attract the rest members' of the organisation notice, as it would be the case, if a conventional (physical) search and seizure was performed [Kudlich, 2007].

The Council of the European Union, shortly after the delivery of the judgement of the German Federal Constitutional Court in the "online search" case, invited the Member-States and the Commission to introduce measures based on case stud-

ies, particularly taking into account technological developments, so as to prepare tools for operational use, such as "facilitating remote searches if provided for under national law, enabling investigation teams to have rapid access to information, with the agreement of the host country" [see Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime, 2987th Justice and Home Affairs Council meeting, Brussels, 27-28 November 2008] [Abel 2009].

## Factual and technical background

Such secret measures were in the recent past performed in isolated cases –fewer than ten per year, according to the Government of the Land– by federal authorities without a specific statutory empowerment and, thus, were temporarily ceased, when the Federal Court of Justice (Bundesgerichtshof) ruled that the Code of Criminal Procedure (Strafprozessordnung - StPO) did not currently provide a sufficient legal basis for their execution (see Decisions of the Federal Court of Justice in Criminal Cases [Entscheidungen des Bundesgerichtshofs in Strafsachen - BGHSt] 51, 211) [Abel und Schafer, 2009].

The political debate in Germany –starring the most outspoken proponent of the measure, Federal Minister of Interior Schäuble and his sceptical opponent, Federal Minister of Justice Zypries– was conducted in a remarkably lively and sometimes witty manner (see the frontispiece of the former's interview in newspaper Handelsblatt of 05.04.2007: "Terrorists do not communicate by carrier pigeons!" [Holzner, 2009]).

Online search is technically feasible via the installation and subsequent activation –usually by sending to the computer concerned an e-mail allegedly originating from a state agency beyond suspicion– of a Trojan horse (e.g. the so-called Root-kits) or a back-door programme. If, for instance, the person concerned uses a program for receiving real-time stock market information, then the Trojan horse is embedded therein and, hence, the law enforcement agency is facilitated to transfer and review of the data existing in the storage medium of the computer, while the user's account is connected to the Internet (online) [Abel and Schafer, 2009]. As the Court has argued, "insofar as such [ongoing Internet communication] is encrypted as it takes place –this is in particular frequently the case with speech telephony– it can only be effectively monitored at the terminal" [par. 11].

A Trojan horse –a malware that appears to perform a desirable function for the user (e.g. tool or game) but instead facilitates unauthorized access to the user's computer system– can thoroughly monitor and ab intra manipulate the communication of the host computer with peripherals, such as monitor, keyboard, or even smart-card readers. Such a malware is suited to erase its digital traces

immediately after the successful performance of its attack, for example by self-deleting [Federrath, 2009].

## Outline

Twenty five years after its landmark judgement in the National Census Case (Volkszählungsurteil) and the establishment of the right to "informational self-determination" [Mitrou, 2009], the Court gave birth to a new fundamental right in the field of information technology on the occasion of testing the constitutionality of the relevant provisions of the North-Rhine Westphalia Constitution Protection Act [Gesetz über den Verfassungsschutz in Nordrhein-Westfalen - VSG NRW] explicitly authorising the competent intelligence authority to engage in secret infiltration of information technology systems.

The Court concluded that the impugned provisions violate the general right of personality in its particular manifestation as a (rather long-winded) fundamental right to the guarantee of the confidentiality and integrity of information technology systems. According to its ruling, the above manifestation protects individuals against intrusion in information technology systems, insofar as the protection is not at all or not adequately guaranteed by other fundamental rights, such as in particular the guarantee of the secrecy of telecommunications or the guarantee of the inviolability of the home, as well as by the right to informational self-determination.

Covert measures in a state based on the rule of law should always be the exception and, likewise, a special justification is required thereof, since, due to the lack of knowledge of the individual concerned of the ongoing procedure, he or she cannot influence by his conduct the course of the investigation.

In respect to its considerable burden of intrusiveness, the secret infiltration of an information technology system by means of which the use of the system can be monitored and its storage media can be read, is constitutionally only permissible, if factual indications exist of a concrete danger to a predominantly important legitimate interest. Predominantly important are the life, limb and freedom of the individual or such interests of the public, a threat to which affects either the basis or continued existence of the state or the basis of human existence (e.g. the functionality of major parts of existence-ensuring public supply facilities). Further, the preventive measure can be justified even if it cannot be ascertained with sufficient probability that the danger will arise in the near future, insofar as certain facts indicate a danger posed by specific individuals to the above predominantly important legitimate interest on a case-by-case basis. This measure must in principle be placed under the reservation of a judicial order. The statute authorising

such an intrusion must contain precautions in order to protect the core area of private life.

In a nutshell, (a) the challenged provisions are not compatible with the principle of the clarity and determinedness of provisions, insofar as the factual preconditions of the regulated measure cannot be sufficiently derived from the statute, (b) the requirements of the principle of proportionality in a narrow sense are not met, since the measures provided for in this norm entail interferences with fundamental rights which are so intensive, that they are disproportionate to the public interest of investigation emerging from the regulated occasion for the encroachment, and (c) the intrusive norms do not provide any suitable procedural precautions –i.e. a judicial order or an equivalent (in terms of independence and neutrality) control mechanism– to protect the inviolable core area of private life.

The new provision of § 20k par. 1 of the "BKA Act" (Act on the Federal Criminal Police Office [Bundeskriminalamt] and the Co-operation between Federal and State Authorities in Criminal Police Matters") authorises the aforementioned state agency to perform "online searches" as a preventive counter-terrorism measure. The law-maker has broadly adopted the encroachment's normative preconditions verbatim from the verdict of the First Senate [Bäcker 2009].

## The "loophole-filling" function of the general right of personality

As the First Senate has ruled, a new anonymous fundamental right is established "in particular in order to counter new types of endangerment which may occur in the course of the scientific and technical progress or changed circumstances" [par. 169]. Previous typical examples of the Court's creative law-making function, via the "loophole-filling" function of the general right to personality, are also the right of reply to the media [Recht auf Gegendarstellung im Presserecht], the right to know one's origins [Recht auf Kenntnis der eigenen Abstammung] and the entitlement to rehabilitation [Anspruch auf Resozialisierung] [Manssen, 2009]. As regards the current case, the Court concluded that the existing array of constitutional weapons does not adequately take account of the need for protection arising as a consequence of the unprecedented development of information technology systems.

### *The guarantee of the inviolability of the home*

The "online search" would not only be constitutionally, but also law-politically short-lived, if it was to fall within the concept of the guarantee of inviolability of the home (Article 13 of the Basic Law): the lack of the majority necessary for the amendment of the relevant provision of Basic Law, so that the latter encom-

passes not only the physical but also the remote interference with the sanctity of the home, was the substantial ground underlying the Court's reasoning that "the location of the system is in many cases of no interest for the investigation measure and frequently will not be recognizable even for the authority. This applies in particular to mobile information technology systems such as laptops, Personal Digital Assistants (PDAs) or mobile telephones" [par. 194]. Moreover, the spirit of the guarantee of the inviolability of the private dwellings is the right to be let alone; yet, the use of information technology systems serves just the opposite purpose, namely the communication with the outside world [Lepsius, 2008].

### *The guarantee of the secrecy of telecommunications*

The court has declared that "the fundamental rights protection provided by Article 10 of the Basic Law however does not cover the content and circumstances of the telecommunication stored subsequent to completion of the communication in the sphere of a subscriber, insofar as he or she can take their own protective precautions against secret data access. The specific dangers of spatially distanced communication, which are to be averted by secrecy of telecommunication, do not then continue to apply to such data" [par. 185]. The protection of the secrecy of telecommunications ends at the exact moment the message arrives to the receiver and the transmission process is complete [Lepsius, 2009].

### *The right to informational self-determination*

Insofar as the citizens reckon on the fact that information technology systems are monitored on a large scale, the collective confidence in the information technology –which is of massive social and economic interest– is inevitably tempted. Therefore, the new fundamental right meets the need of protection of the individual's information technology system as a particular safeguarded area of privacy. The starting point of the constitutional protection is the system itself –any electronic system which is used for data processing: a definition intentionally open and technically neutral– rather than the stored data therein [Bäcker, 2009]. That is the prevailing reason, why online search does not fall into the scope of protection of the right to informational self-determination.

Moreover, the Court has argued that "the right to informational self-determination does not fully consider elements of personality endangerments which emerge from the fact that the individual relies on the use of information technology systems for his or her personal development and, in such instances, entrusts personal data to the system or inevitably provides such data already by using the system. A third party accessing such a system can obtain data stocks which are potentially extremely large and revealing without having to rely on further data collection and data processing measures. In its severity for the personality of the person

concerned, such access goes beyond individual data collections against which the right to informational self-determination provides protection" [par. 200]. This ruling reflects the Court's tendency to narrow the scope of the traditional data protection fundamental right, so as to make room for creating a new guarantee –as if the Court no longer trusted the right to informational self-determination to deal with the Internet technicalities and the privacy infringements related thereto [Lepsius, 2008).

## The case-law of the European Court of Human Rights

Although the concept of an "information technology" right is expressis verbis unknown to the European Court of Human Rights, yet the broad interpretation of the notion of the right to respect for private life, enshrined in Article 8 of the European Convention on Human Rights, leaves considerable space for the recognition of confidentiality and integrity of information technology systems as important principles underlying such interpretation [Uerpmann-Wittzack, 2009].

In the leading case of *Copland v. the United Kingdom* [no. 62617/00, § 41, ECHR 2007-IV] the Court acknowledged that "the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8".

Further, in the case of the *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (no. 62540/00, § 86, 28 June 2007) the Court criticised "the apparent lack of regulations specifying with an appropriate degree of precision the manner of screening of the intelligence obtained through surveillance, or the procedures for preserving its integrity and confidentiality and the procedures for its destruction".

## Critical assessment

According to some legal commentators this right is nothing but a "constitutional fireworks" or an "empty conception" [Bäcker, 2009]. Others contend that the existing constitutional framework of informational self-determination was dogmatically as well as methodologically sufficient enough to preserve privacy under the new pressures from surveillance technology [Manssen, 2009], while some compare the judicial formulation of the aforementioned guarantee to the establishment of the right to privacy by the US Supreme Court in 1970's [Lepsius, 2008].

Confidentiality means that information is accessible only to authorised persons, while authorisation refers to a deliberately set up technical access possibility. Likewise, Solove [2008] argues: "confidentiality [...] consists of sharing the in-

formation with a select group of trusted people". On the other side, integrity means that information is complete, accurate and up-to-date, or it is clearly noticeable that this is not the case, so the Court, "by the system being accessed such that its performance, functions and storage content can be used by third parties; the crucial technical hurdle for spying, surveillance or manipulation of the system has then been overcome" [par. 204]. However, the Court has not guaranteed the third goal of data protection, i.e. availability [Verfügbarkeit] of information: the latter is accessible by the aforementioned authorised persons whenever and wherever there is a need thereof [Hansen and Pfizmann, 2008].

As the Court has observed, new endangerments of personality "emerge from the fact that complex information technology systems, such as personal computers, open up a broad spectrum of use possibilities, all of which are associated with the creation, processing and storage of data. This is not only data which computer users create or store deliberately. In the context of the data processing process, information technology systems also create by themselves large quantities of further data, which can be evaluated as to the user's conduct and characteristics in the same way as data stored by the user. As a consequence, a large amount of data can be accessed in the working memory and on the storage media of such systems relating to the personal circumstances, social contacts and activities of the user. If this data is collected and evaluated by third parties, this can be highly illuminating as to the personality of the user, and may even make it possible to form a profile" [par. 178].

Setting aside the fact that collection and evaluation of personal information are the privileged field of informational self-determination right –and thus the latter's exclusion from legal instruments adequate to address the issue of secret infiltration of information technology systems seems rather unjustifiable– the First Senate has further noted that "the performance of information technology systems and their significance for the development of personality increase further, if such systems are networked with one another. This is increasingly becoming the norm, in particular because of the increased use of the Internet by large groups of the population" [par. 174]. According to a famous quotation of Scott McNealy –a legendary character of Silicon Valley– "the Network is the Computer" [Böckenförde, 2003]. Most notably, however, as the Court has declared, "the networking of the system opens to third party a technical access facility, which can be used in order to spy or manipulate data kept on the system" [par. 180]. In other words, protection worthy is per se the potential of networked communication, not even the actual creation of individual data traces [Lepsius, 2008].

Thus, the "information technology" fundamental right encompasses either complex systems, such as personal computers and smart phones, or simple external

storage media (e.g. hard drives or USB-sticks), which, due to their connection with another data medium, constitute a sufficiently complex system overall. Accordingly, the new right protects as well virtual hard drives or network-based application programs [Bäcker, 2009].

In this objective-orientated context –in contradistinction to the subjective structure of the right to informational self-determination– [Lepsius, 2008], the Court has cited as examples of devices that are not to be classified as information technology systems, in the sense of its new case-law, non-networked electronic control systems in household appliances or non multifunctional mobile telephones and electronic appointment pads, insofar as such systems due to their technical construction only contain data with a partial connection to a certain area of life of the person concerned [par. 202, 203]. Thereby, the Court comes up against unsolvable problems of demarcation: How many functions must a mobile telephone fulfil, so that it ranks among worth-protecting information technology systems? Is redial enough, or address book and folder management are additionally required? What about SMS, Bluetooth, camera or MP3 player? Moreover, the ruling fails to provide a convincing argument for the normative differentiation between an electronic diary and a conventional one: "what is offline illegal can not be online allowed, not even for the State" [Mannsen, 2009].

On the other hand, the Court has lamented that "the constitutional requirements as to the concrete structure of the protection of the core area can differ depending on the nature of the collection of the information and the information collected by it. A statutory empowerment to carry out a surveillance measure which may affect the core area of private life, must ensure as far as possible that no data is collected which relates to the core area. If –as with secret access to an information technology system– it is practically unavoidable to obtain information before its reference to the core area can be evaluated, sufficient protection must be ensured in the evaluation phase. In particular, data that is found and collected which refers to the core area must be deleted without delay and its exploitation must be ruled out" [par. 276, 277].

This ruling, addressing the –inherent to information technology and investigative technique– difficulty of an ex ante assessment, whether the information secretly accessed is core-area relevant, is of profound importance for the combating of particular aspects of criminality e.g. child-pornography; indeed, even if the person concerned was under concrete suspicion of possessing child-pornography material, under the Court's recent case-law it was a contentious issue, whether the state agents were justified to open a folder titled "Love letters" [Schmidbauer, 2009].

Moreover, the First Senate has demonstrated that the core area of private life is not an obstacle to secret access of the targeted information technology system, "if for instance concrete indications exist that core-area related communication contents are linked with contents which fall within the goal of the investigation in order to prevent surveillance [par. 281]. As an author vividly asserts, "evidently, the Court entertains the idea that clever terrorists seek that their criminal plans evade the state surveillance by intimate whispers with their sexual partners" [Kutscha, 2008].

## Conclusion and perspective

Information technology has evolved to an autonomous field of performance not only of social or economic activity, but also of new forms of criminal behaviour. Equally, however, information technology constitutes a new, independent field of investigation of network-related delinquency. If the personal computer and the digital information stored therein were until recently the subject of investigation, these have already transformed to a prominent tool therefore [Böckenförde, 2003].

Information Law is the legislator's answer to the technological revolution that has altered –and keeps altering– the reality of life. More than 20 years ago, an influential academic asserted that "despite the incontestable importance of its technical aspects, informatization, like industrialization, is primarily a political and social challenge" [Simitis, 1987]. The legal order, as an instrument expected to provide stability and security to the individuals and society, is hence structurally conservative [Uerpmann-Wittzack, 2009]. Yet, the establishment of a new fundamental "information technology" right –to be more precise, a new sub-group of the general personality right [Hornung, 2009]– by the German Federal Constitutional Court is much more than just "relabeling old wine in new bottles". It rather reflects a comprehensive answer of an Information Law for the 21st Century to the relentless questions raised by the rapid technological development and the privacy concerns inherent therewith.

## References

German Federal Constitutional Court, Judgment of the First Senate of February 27th, 2008 - 1 BvR 370/07, online at http:/www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html/accessed 25.05.2010 (also available in English)

Abel W. (2009), The German "Federal Trojan" – challenges between law and technology, Teutas - Diritto e Tecnologia 2009 (2), 20-32

Abel W., and Schafer B. (2009), The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822, SCRIPTed 6:1 (2009), 106-123

Bäcker M. (2009), Das IT-Grundrecht: Funktion, Schutzgehalt, Auswirkungen auf staatliche Ermittlungen, in: R. Uerpmann-Wittzack (Hrsg.), Das Neue Computergrundrecht, Recht der Informationsgesellschaft Bd. 15, Berlin [u.a.]: LIT-Verl., 2009, 1-30

Böckenförde T. (2003), Die Ermittlung im Netz, Tübingen: Mohr Siebeck, 2009

Federrath H. (2009), Technische Aspekte des neuen Grundrechts, in: R. Uerpmann-Wittzack (Hrsg.), Das Neue Computergrundrecht, Recht der Informationsgesellschaft Bd. 15, Berlin [u.a.]: LIT-Verl., 2009, 53-60

Hansen M. and Pfizmann A. (2008), Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen, in: F. Roggan (Hrsg.), Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Berlin: BWV Berliner Wissenschafts-Verl., 2008, 131-154

Hofmann M. (2005), Die Online-Durchsuchung – staatliches "Hacken" oder zulässige Ermittlungsmaßnahme? NStZ 2005, 121

Holzner S. (2009), Die Online-Durchsuchung: Entwicklung eines neuen Grundrechts, Rechtswissenschaft Bd. 211, Kenzingen: Centaurus-Verl. 2009

Hornung G. (2009), The Online Searching Judgement of February 27th, 2008, in: R. Bendrath/G. Hornung/A. Pfizmann, Surveillance in Germany: Strategies and Counterstrategies, 3-6, online at http://userpage.fu-berlin.de/~bendrath/Bendrath-Hornung-Pfitzmann_Surveillance-in-Germany_2009.pdf/accessed 25.05.2010

Kudlich H. (2007), Zur Zulässigkeit strafprozessualer Online-Durchsuchung, HFR 2007, online at http://www.humboldt-forum-recht.de/deutsch/19-2007/index.html/ accessed 25.05.2010

Kutscha M. (2008), Neue Chancen für die digitale Privatsphäre? in: F. Roggan (Hrsg.), Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Berlin: BWV Berliner Wissenschafts-Verl., 2008, 157-171.

Lepsius O. (2008), Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft, in: F. Roggan (Hrsg.), Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, Berlin: BWV Berliner Wissenschafts-Verl., 2008, 21-56

Livos N. (2007), Organised Crime and Special Investigative Techniques, Vol. I: Dogmatics of Organised Crime, Part (a): The criminological-dogmatic phenotype of organised crime, Athens: Law & Economy - P.N. Sakkoulas, 2007

Manssen G. (2009), Das "Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme" – Ein gelungener Beitrag zur Findung unbenannter Freiheitsrechte? in: R. Uerpmann-Wittzack (Hrsg.), Das Neue Computergrundrecht, Recht der Informationsgesellschaft Bd. 15, Berlin [u.a.]: LIT-Verl., 2009, 61-72

Mitrou L. (2009), The Commodification of the Individual in the Internet Era: Informational Self-determination or Self-alienation? in: M. Bottis (ed.), Computer Ethics: Philosophical Enquiry. Proceedings of the 8th International Conference, Ionian University, Corfu, June 26-28, Athens: Nomiki Bibliothiki, 2009, 466-484

Schmidbauer W. (2009), Moderne Technik, das Bundesverfassungsgericht und die Polizei – Vorstellungen zur Polizeiarbeit in Computerzeitalter, in: R. Uerpmann-Wittzack (Hrsg.), Das Neue Computergrundrecht, Recht der Informationsgesellschaft Bd. 15, Berlin [u.a.]: LIT-Verl., 2009, 31-51

Simitis S. (1987), Reviewing privacy in an information society, 135 U. Pa. L. Rev. 707 (1987)

Solove D. J. (2009), Understanding privacy, Cambridge: Harvard University Press, 2009

Uerpmann-Wittzack R. (2009), Der Schutz informationstechnischer Systeme nach der Europäischen Menschenrechtskonvention, in: R. Uerpmann-Wittzack (Hrsg.), Das Neue Computergrundrecht, Recht der Informationsgesellschaft Bd. 15, Berlin [u.a.]: LIT-Verl., 2009, 99-109

# Right on privacy in the Republic of Serbia

**Nataša Tomić & Dalibor Petrović**

## Introduction

Fast technological development presents a challenge for the protection of personal data and the right on privacy. In this paper we have analyzed privacy protection and examined domestic and European legal acts on the privacy protection. We have analyzed privacy protection on the Internet with special regards to the most popular social networking sites (SNS).

One of the most discussed topics today, when we speak about social consequences of the new information communications technologies (ICT) utilization, and first of all Internet is certainly the problem of privacy protection of users of these technologies. Unexpected high number and speed of the data flow which those technologies have brought the danger of different forms of abuse of data transferred through ICT. That this is not the one of many groundless fears, in the best way testify the series of recommendations and guides for the protection of privacy on Internet made by different regulatory bodies throughout the world. Many public protests, different petitions, as well as official legal actions for endangerment of privacy of users of the most popular social networking sites testify about that.

Anyway the sale of personal computers in the world according to American media, has grown in the first quarter of the year 2010.[1] for 27,4% in relation to the same period of the last year because of the increased demand in Europe, Africa and in the Middle East. In our country the sale of computers has also grown. In Serbia, according to the data of the Institute for statistics of the Republic of Serbia, 46, 8% households have computer[2], and in 2006. that percentage amounted to 26,5%. While during 2006, the percentage of households that have access to Internet was 18,5%, that number has been gradualy increased and in 2009. the 36,7% households in Serbia had access to Internet.[3] Today still one-third of Serbia does not have access to fast Internet, although surfers in our country more and more follow the world trends. In the meantime, in the world in June 2009. in the research Centre Jilich in Germany the supercomputer with power of 50.000 personal computers was solemnly set in motion. It was called the Jugene[4] and it is the fastest in Europe, after Roadrunner-and Jaguar-a in the United States of America. It will be used for different purposes for example for the weather forecast and for the research of the Universe.

In the Republic of Serbia many legal acts deal with the protection of privacy of individuals and groups, and the expanded regulatory framework for the fight against these kinds of abuses exists. Additional problem represents that, by voluntary giving away of confidential personal data in their profiles, users became accomplices in these abuses. If you are not sure that you will do really well, try, at least, not to make harm, wrote A. Huxley (1894-1963).

Recently the public has been informed about many abuses, so we also found out that for Google the privacy is not a holy place. It was announced that famous American company illegaly took data from the users in Germany[5], so the question is if the same thing is happening here in Serbia.

Finally, in this paper are emphasized different recommendations for the prevention of personal data abuse.

## On the legal regulation of the right on privacy

it is important to stress that the right on privacy is one of the basic human rights. "Right to be left alone" means storing of smb's data secrecy, unless, there is an obvious need to reveal these data. This question requires carefull access in many areas (especially in the area of health and finances, but also on the occasion of Internet utilization). Riley T. has offered proposals for the protection of the man's right to be left alone [1]. These proposals are:

- internal use of information technology, development of personal policy that will protect rights of employees on privacy, contrary to the right of public to find out;
- adoption of laws and carring out of the policy which will explain the right on access of each individual organization to certain information on individuals;
- provision of mechanisms for removal or change of incorrect or obsolete information; and
- acceptance of new technology, building of the system of privacy protection immediately, and not after the problem appears.

In the Republic of Serbia many legal acts deal with the privacy protection of individuals and groups, so it may be concluded that there is expanded regulatory framework for the fight against those forms of abuse.

The Constitution of the Republic of Serbia[6] adopted in year 2006. guarantees the protection of personal data, and collection, keeping, processing and utilization of personal data is regulated by law.

The utilization of personal data besides the purpose for which they were collected is prohibited and punishable in accordance with law, except for the needs of the management of criminal proceedings or the protection of security of the Republic of Serbia, in the manner predicted by law. Everybody has the right to be informed about the data collected on his/her person, in accordance with law, and the right on legal protection because of their abuse.

The Constitution of the Republic of Serbia guarantees the inviolability of correspondence and other means of communication, and derogations are legal only in fixed time and on the base of the court decision, if they are necessary because of the management of criminal proceedings or the protection of security of the Republic of Serbia, in the manner predicted by law.

By the Law on the protection of personal data[7] are regulated conditions for collection and processing of personal data, procedure in front the body competent for protection of the data on person, security of data, records, taking out of data from the Republic of Serbia and supervision over the enforcement of the law. Protection of personal data is ensured to each natural person, disregarding citizenship and residence, race, age, sex, language, religion, political and other conviction, nationality, social origin, financial status, birth, education, social situation or other personal qualities. The aim of this law is to ensure to every natural person, in connection with the processing of personal data, realization and protection of the right on privacy and other rights and liberties.

With right on privacy and other personal rights deals also the Law on free access to information of public importance[8] which predicts that authorized body will not provide for realization of the right on access to information of public importance to the claimant, if by that would be injured the right on privacy, the right on reputation or any other right of the person to whom asked information personally refers to, unless:

1) if person agreed with that; 2) it is the person, phenomenon, or event of interest for the public, and expecially if it is about the holder of state or political function and if information is important with regard to the function that person performs; 3) if it is about the person who by his/her behavior, especially in connection with private life, gave the pretext for request of information.

Law on telecommunications of the Republic of Serbia[9] in performance of the control over carring out of activities in the area of telecommunications predicts authorization of the Agency to check, in addition to everything else, acting of public telecommunication operators in relation to duties predicted by this law in the area of privacy and security of information and undertakes measures to eliminate fixed omissions in acting of operator.

Licence, in addition to other data and conditions, contains also rules on the protection of personal data and privacy, which are specific for cerain area of telecommunications. Public telecommunication operator is obliged to undertake appropriate technical and organizational measures in order to provide for confidentiality and security of his services and it is prohibited to him to give information on contents, facts and conditions of messages transmission, except the minimum necessary for offering the services on the market or in the cases predicted by law. Data on the traffic related to individual users and which are being processed in order to establish connection, public telecommunication operator may keep and process only in the scope necessary for invoice to the user.[10] All activities and utilization of devices which endanger or disturb privacy and confidentiality of messages which are transmitted through telecommunication networks are prohibited, except when there is a consent of the user or if these activities are performed in accordance with the court order issued in accordance with law. Public telecommunication operator is obliged, as part of the system, to form, at his own expense, subsystems, devices, equipment and installations for by law authorized electronic supervision of certain telecommunications. Users of public telecommunication services or public telecommunication networks have the right on undisturbed utilization and high-quality public telecommunication service, as well as the right on privacy and security of information.

Besides mentioned laws, the Government of the Republic of Serbia during October 2006. adopted also two Strategies which, in addition to everything else, treat also the area of the protection of privacy. Strategy for development of telecommunications in the Republic of Serbia from year 2006. to year 2010.[11] predicts that working of national regulatory bodies includes also the protection of privacy, protection of users traffic, data on location, prevention of unwanted communication.

Besides the right on undisturbed utilization and high-quality public telecommunication service, for users of public telecommunication services or public telecommunication networks is necessary to ensure also the right on privacy and security of information.

With aim to strengthen all aspects of security and safety of telecommunication sector the provision of multiple levels of protection of telecommunication systems from malicious attacks is performed, i. e. telecommunication systems must be safe enough to build trust of clients in electronic payment and transactions. In Strategy for development of information society in the Republic of Serbia[12] is pointed out that electronic networks must be ensured from hackers and viruses and must be safe enough in order to build trust of clients in electronic payment,

and the issue of security must be balanced with the possible violation of privacy of citizens.

Government as the national regulator is responsible for setting of national rules for utilization of technology. They are also made of national standards which regulate privacy and security of data, like laws related to access to sources of information, national and international, including also the Internet. The main aim of the activity in the area of security infrastructure is to define and build mechanisms, like public key infrastructure, that will provide for the protection of privacy of citizens, make electronic transactions safe and increase trust in e–government. Solutions that have to be developed should be in accordance with the international standards in this area.

At the end, it is important to mention that at the moment the public hearing on the new Law on electronic communications[13], that should replace Law on telecommunications of the Republic of Serbia is under way. In contrast to the existing Law on telecommunications in the Draft of the Law on electronic communications the area of users privacy protection is mentioned in the basic provisions as well as in the principles of the new law. Besides that, one whole chapter of the Draft of the Law (XIV) is devoted exclusively to the users privacy protection and the security of electronic communications networks and services. However, the lack of regulation related to the privacy of data on Internet is still noticeable, so the existing law proposal should be supplemented in that direction.

When we speak about European legislation, we have examined few key Directives which regulate the area of protection of data security in electronic communications, and of special importance is 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 movement of such data.[14] Free movement of goods, persons, services and capital requires not only that personal data freely circulate from one member state to another, but also that the personal rights of individuals are protected. Progres in information technologies significantly facilitated the processing and exchange of these data. However, different levels of protection of rights and liberties especially the right on privacy, taking into consideration the processing of personal data collected in the member state, can prevent the transmission of those data from the territory of one to the territory of another member country. In order to remove obstacles for exchange of personal data, level of protection of rights and liberties of individuals with regard to processing of such data must be eqivalent in all member states. Principles of protection should be applied on the processing of personal data of individuals whose activities are regulated by laws of the Community, while the processing of data performed by natural persons in carring out of activities of excusively

personal and family nature, like correspondence and keeping data on addresses, is excluded.

In accordance with Directive 95/46/EC member states protect the basic rights and liberties of natural persons, and especially their right on privacy with regard to the processing of personal data. Directive will not be applied on processing of personal data which concerns public security, defence, state security, including economic welfare of states, when processing relates to the issues of state security, as well as the activities of the state in the area of criminal law. This Directive will not be applied also on the processing of personal data of natural persons during exclusively personal or family activity. Member states will define more precisely, in the limits of provisions determined by this Directive, conditions under which the processing of personal data is legal.

Because of intensive development of telecommunications a need to further strengthen and state precisely conditions of. disposition, storing and distribution of personal data appeared, so during year 1997. the Directive of the European Parliament and Council on the processing of personal data and the protection of privacy in telecommunication sector (Directive 97/66/EC)[15] was adopted. However, the key Directive which is completely dedicated to the protection of privacy in the domain of electronic communications is so-called Directive on e-privacy or under the full title The Directive on Privacy and Electronic Communications 2002/58/EC.[16]

One of its main roles is to harmonize provisions of the member states necessary for provision of the same level of protection of basic rights and liberities, and especially the right on privacy, with regard to the processing of personal data in the sector of electronic communications, as well as the provision of free transmission of these data, equipment for electronic communication and services in the Community. This Directive is applied on the processing of personal data in connection with the provision of services of electronic communications in the networks of public communications inside the Community. The duty of provider of the service of electronic communications is to take appropriate technical and organizational measures in order to provide for security of his/her services, if it is necessary in connection with provider of the network for public communications, and with regard to the security of the network. In the case of special risks of disturbing of the network security, the provider of the service of electronic communications has to inform subscribers on the risk and when the risk is out of the spectrum of measures taken by the provider, on the possible means, pointing to the possible expenses.

By this Directive, in addition to everything else, is regulated the issue of sending of unwanted electronic mail (spam) in the European Union. The question is

in what extent the protection assigned to subscribers in this Directive should be spread on the corporative subscribers? For example, according to the valid regulations when the enterprise provides for mobile phones for its employees for business purposes there is no right to prevention of unwanted marketing calls, because the subscriber is the enterprise, and not the employee. Regulations are formulated in such a way that in special circumstances the wishes of users of the service (legal person) can prevail the wishes of individual users. In order to get consent for the data processing, providers should offer to users clear information that will enable them to get explanation of presumable consequences for them in the case of consent.

However, since the phenomenon of on-line social networking appears and intensively spreads after the adoption of mentioned directives, the need emerged for making additional sub-laws that will especially deal with protection of data privacy on web platforms for social networking (PSN). In that sense, the most important act that we shall mention here is the Opinion 5/2009 on on-line social networking adopted on the 12th of June 2009. that deals with the manner how functioning of the social sites on the network can fulfill request of the European Union legislation on the data protection.[17] It is, first of all, intended to give guidelines to providers on the measures that should exist in order to provide for harmonization with the European Union laws. The Opinion underlines that the service giver and, in many cases, third persons as service providers, controllers are responsible toward the users. It is emphasized that the great number of users is moving inside the purely private sphere, and in such cases rules that regulate the management of data controllers are not applied.

## Privacy policy on the sites for social networking

The problem of the privacy protection on SNS is the subject of many research studies, discussions and recommendations of wider public, as well as of scientists, governmental and non-governmental organizations.

The reason for such great interest for this topic lies down in the fact of unimagined speed of increase of the number of people who, more or less, ex gratia share information of different levels of confidentiality through SNS.[18] What concerns is the fact that information stored on SNS can forever stay there and like such be available to different individuals and interested groups and organizations. Besides that, information, once released through the network, is instantly transmitted and becomes globally available to everybody.

Additional problem, on which points out the majority of analysts who deal with the problem of the data privacy protection on Internet, represents the fact that users on their initiative and ex gratia give information on themselves (name and

family name, addresses, phone numbers, photographies, etc.), and that in the process think little on the consequences of such acting. For example, Gross & Acquisti in their research study show that almost 82% of active users of Facebook reveal confidental information on themselves like the date of birth, number of mobile phone, address, political and sexual orientation and the name of partner [2]. Similar results reached Young & Quan-Hasse investigating the behavior of students in Canada [3]. The results show that incredible 99,35% of students use real name in their profiles; 97,4% cite the name of school they attended; 92,2% the date of birth; 83,1% e-mail address; 80% the name of the town they live in.

In addition, almost all students put their photographies on profiles (98,7%) and photos of their friends (96,1%). However students are little more careful when it comes to giving the right address (that does only 7,9%) or the number of mobile telephone (10,5%).

Such great frankness of SNS users is stimulated by the providers of these services who encourage the publication of personal data by creating illusion of their complete safety. That situation is just not so innocent, as probably thinks the majority of SNS users, testify many analysis, guides and recommendations with aim to regulate better this sphere of social activity. But, the most of all, on the possibility of data abuse, testify also concrete doubts, public petitions, and even lawsiuts against the most popular SNS, Facebook.

The first great discussion on the topic of manipulation with personal data of facebook users, happened after the introduction of the contraversial system for advertising »Beacon». Introducted in November 2007, this service was set up to record the activity of all Facebook users on Internet (purchase, application for different services, etc.) and then forward these information to the list of friends from the profile of this person. The idea was to advertise companies on a more personal, personalized way, by recommending friends the services and products that their friends use.

After the lawsuit and under the pressure of users complaints, only two months later, Beacon service with apologies of the founder Mark Zuckerberg[19] becomes optional, and in September 2009. it was published that it will be completely abolished.[20]

During the year 2009. Facebook was two more times the subject of wide discussion and public complaints. New controversy (February 2009.) caused the announcement by the Facebook, that their policy concerning the privacy of data will be changed. This announcement especially excited public by one paragraph by which Facebook reserves the right to possession of users personal data even in the case when the user disables his/her profile and erases data from it. However,

after many protests and wide campaigns around the world and the threat of a lawsuit, the creators of the Facebook were once more forced to give up from intended changes.[21]

Much more serious consequences for the problem of the Facebook privacy policy caused the lawsuit of one Canadian non-governmental organization dealing with the Internet policy and public interest (Canadian Internet Policy and Public Interest Clinic - CIPPIC) sent to the »Office of the Privacy Commissioner»-(OPC). This organization submitted a complaint on the Facebook users data privacy policy on several levels [4]. From the complaint for unauthorized collecting («phishing») of data on birth of users, to the complaining on unauthorized giving of users personal data to the third persons for the purpose of advertising. In the response to the complaint OPC has made several reports and during March 2009. gave 20 recommendations related to the removal of the noticed irregularities in the connection with the privacy policy of their users to the Facebook [5]. As the result of all this, the Facebook corrects one part of its privacy policy related to the standard / default/ adjustment of the security mechanisms on the profile, as well as in the field of advertising, but the important part of the complaints concerning the application of third persons, deactivation and deleting of profiles, profiles of deceased users and personal information of non-users, remained unsolved till today.

## Recommendations for reduction of the security risks on the sites for social networking

just problems like the so far presented, created the need for adoption of appropriate standards when the privacy of SNS users data is in question. One of the most voluminous analysis of this problem was made by the European Network and Information Security Agency - ENISA. In its Report «Security problems and recommendations for online social networks» from 2007. the following threats, divided in four categories [6] are cited:

- Threats for privacy:
- Traditional danger for networks and the information security;
- Threats for identity;
- Social threats.

In accordance with the identified threats ENISA gives recommendations and contra measures for increasing of the security level of persons and data and that means:

- *Recommendations in the area of Governmental regulatory policies (for example,* raising of conscience and educational campaigns),

- *Recommendations for providers and their business policy (for example,* establishing of the appropriate settings of profiles that will really protect the privacy of users),
- *Technical recommendations (for example,* providing for better control of privacy during searching of personal data)
- *and Recommendations in the area of research and standardization.*

One year later (2008) "International working group for data protection in telecommunications", so called Berlin group, published its Report and Guide on the protection of privacy, for the creators of SNS and users of these applications [7]. In this report, more famous by the name Roman Memorandum, the risks for privacy and security of SNS users are especially emphasized, and in accordance with identified risks, Working group made recommendations for these who regulate, give and use services of social networking.

- For regulatory bodies:

1. Make possible the right on utilization of pseudonyms instead of the real names;
2. Provide for service providers who are sincere and clear in the respect of information needed for the basic service, so the users can judge if they are going to give those information, and possibility that users may not allow any secondary utilization of their data, especially not for targeted marketing;
3. Introduction of the duty of informing on breaking into the SNS users data;
4. Revision of the existing regulatory framework in regard to the management by personal data published on SNS;
5. Integration of the privacy issues into the educational system.

- For providers of services of social networking

1. Transparent and open informing of users;
2. Introducing the posibility of creation and utilization of profiles under pseudonym;
3. Keeping the promises given to users;
4. Default settings which are directed to privacy protection;
5. Improving the control of users over utilization of their data from profiles;
6. Introducing of appropriate mechanisms for users complaints management;
7. Improving and maintaining the systems for information security;

8. Finding and/or further advancement of measures against illegal activities, like spaming and theft of identity;
9. Offering of encrypted connections for maintainance of profiles;
10. Providers of social networking services, who operate in different countries or globally, have to respect standards on privacy protection everywhere they offer their services.

• For users:

1. Be careful, think twice before you publish the personal data in your profile;
2. Think well before you use your real name. Use pseudonym;
3. Respect privacy of others;
4. Be informed on the service provider;
5. Use settings which enable your privacy protection;
6. Use different identification data (user name and password) from those that you use on other sites;
7. Use possibility to control how the service provider uses your personal data;
8. Pay attention to the behavior of children on Internet and especialy on SNS.

When we speak about recommendations we should also mention here the research of OPC conducted during 2008 and which after identification of the more or less known threats on SNS, gives even 71 recommendations for the improvement of privacy protection of their users [8].

In already mentioned opinion (**Opinion 5/2009**)[22] there are series of recommendations with aim to increase the data security on PSN. The basic recommendations relate to the duties of service providers to harmonize with Directive on the data protection and to confirm and strengthen the rights of users. Very important is that service providers notify users about different purposes for which they are processing personal data.

The special attention service providers should pay on the processing of personal data of minors. It is recommended that users may use pictures and information on other individuals, but with consent of that individual and it is considered that service providers also have the duty to give advices to users of services on the right on privacy of other persons. To the providers of services on PSN, as well as to the third persons who offer different applications is suggested that it is necessary to notify users on their identity and different purposes for which they are processing personal data in accordance with the provisions of article 10. of the Directive on data protection including, but not only:

- utilization of data for direct marketing purposes;
- possible sharing of data with certain categories of third persons;
- review of profiles: their creating and main sources of data;
- utilization of sensitive data.

It is recommended that service providers on social networks provide for appropriate warnings to users on the risks for their privacy and the privacy of other persons when taking over information from the network. Users should be also reminded that taking over of information on other individuals may violate their privacy and the right on data protection.

It is necessary to advice users of services on social networks that if they want to take over photos or data on other individuals, that should be done with their consent. Data which reveal ethnic origin, political attitude, religious or philosophical beliefs, membership in unions or data on health or sexual orientation are considered sensitive. Sensitive personal data can be published on the Internet only with explicit consent of the subject to whom this data refer to or if the subject himself/herself made those data public.

When user does not use the service in certain time period, the profile should become inactive, i. e. invisible for other users or external world, and after certain period the data from the abbandoned account should be erased. Service providers on social networks should inform users before under taking of these steps with all means they have on disposal. Access and correction as the rights of users are not limited only to users of the service, but to every natural person whose data were processed. The members of social networks and those who are not must have means to perform the rights of access, corrections and erasing.

The basic homepage of the service provider's sites on the social networks should clearly point at the existance of the «service for settling complaints» founded by the provider because of the data protection and settling of the question of privacy and complaints of members and of those who are not.

## Experiences of serbia

participation of the Internet connection is the biggest in the capital city of Belgrade and it amounts to 48,6%, in Vojvodina 37,9%, in Central Serbia 30,50%, according to the data of the Institute for statistics of the Republic of Serbia. Of course, the significant differences are present between city and village settlements all over the country.[23]

Working group of the Register of the national Internet domains of Serbia has started to collect proposals, in order for Serbia to get the network address in

Cyrillic letters, what will provide for creating and searching of the Internet sites on Vuk's[24] Cyrillic writing. As the proposal the most often appears: **срб.** In October 2009 in Seul was adopted the decision that the languages which are not written in Latin letters get their Internet domains. From the 16th of November 2009 the acceptance of new domains proposals[25] has started and till now 19 countries have delivered their proposals.

When we talk about Serbia, certain legal regulation, that should regulate the problem of privacy protection of persons and data on Internet, exists, but, besides that, in our public so far we have not heard for the lawsuits in this area. When we talk about utilization of SNS, Serbia is the first in the region by the number of registered profiles on Facebook with even million of these profiles. This number should not be mixed with the real number of SNS users which is certainly smaller, but nevertheless tells that this phenomenon is widespread among domestic users of Internet. At the other side, in contrast to the good results achieved in the field of networking, Serbia is at the bottom when we talk about the trade by Internet. Even 87,4% of Internet users in Serbia were never shopping by Internet [9], what points to the fact that SNS are not understood as potentially risky for users in the contrast to trading on Internet.

In Serbia till today research studies dealing with the protection of privacy on Internet are rare. Of course, we should mention one of the pioneer's research studies on this subject conducted by Popović V. during 2001. on more than 1073 interviewed persons.[10] Already in this early stage of Internet utilization in our country, as the results of Popović's study show, users of that time have demonstrated unexpectedly strong willingness to leave their personal data on Internet. Here we should emphasize that at that time SNS did not exist, so their frankness can not be understood as the expression of some kind of fashion, but more likely as the absence of expressive conscience on potential dangers watching for on Internet. So, even 75,7% of interviewed persons say that they would leave data on the year of their birth, profession (82,3%), sex (92,1%), etc. on Internet. One half of the interviewed persons is ready to reveal name and surname and e-mail, while even 22,4% would also reveal the home address, and little less the phone number (15,2%) too. We have to add also 14% of those who are ready to leave so confidential fact as it is the identification number on some of the sites.

Recent research directly dealing with SNS was conducted during 2008. by Jovanović S. with associates and it concerned student's population in Serbia and their utilization of Facebook and My Space.[11]. The research was conducted on the sample of 1664 interviewed persons and the reached results were similar to those related to their colleagues on the West. The most interesting finding is that only 5% of users keep their profile hidden for all users, while even 56% of

students allow that their profile is visible by all Facebook users, no matter if they are on the list of their friends of not. The number (35%) of those who reveal full name and surname, date of birth, e-mail address or phone number on their profiles is not small.

Results of these studies show that Serbia, when we talk about behavior of their Internet users is part of the global world. Although we are shopping far less by Internet, what may be also shows unjustified fear from the risk of such form of trading, from other side the great popularity of SNS with our users and their unconcern for the possibility of manipulation with personal data shows that in the future it will be very important to work on the raising of conscience on the risks that such behavior on SNS brings.

## Conclusion

As we have already mentioned in our country till today research studies on the protection of privacy on Internet were rare.

The social networking sites, in our opinion, are paradigm of the risky society of today. Ad captum, having in mind that Internet draws up the plans for society in its virtual shape, it is understandable that by anlogy in the virtual world of Internet are projected also the risks of the real world. However, through this paper we tried to demonstrate that, before mentioned, risks for privacy of persons and data can be reduced on several levels.

Take care, never do anything against your will, wrote Seneca.[26]

On the legislative plan solutions that could enable uninterrupted exchange of information and transactions by Internet should be offered. It is necessary to start with utilization of the electronic signature, allow identification and authorization of participants in transaction, operations with credit cards and establish jurisdiction over Internet transactions. Along with that, it is necessary to insure protection of the personal data and privacy, transfer of information through international systems, cryptographic protection and protection of users from insulting, illegal and unwanted Internet contents. In our country there are still no fundamental rights on video-supervision. The Commissioner for informations of public importance and data protection of Serbia expressed his concern, because the theft of identity has dramatic proportions in the whole world.

That what can be done already now is raising of awareness of the users of the social networking sites, but not through calls for boycott of SNS, because these calls will not have results, but through the permanent promotion of personal care for data given to others at disposal, in extent in which the individual worries not to lose identity card or his mobile phone. When users understand that the

personal data which they leave in the virtual space of Internet are very real and that consequences of their abuse can reflect on their real, and not virtual profiles, then they will be more careful, in the matter to whom these data can be entrusted for keeping, and to whom not.

Providers of the social networking services should also, besides the wish for getting the profit, think about those persons who indirectly bring that profit, i. e. on their users. If the mechanisms for personal data protection are not raised on the level of the really safe stay on SNS, users will start to look for alternative ways for their connection.

## Endnotes

1. The highest sale has realized the company »*Hewlett* Packard « and that is 15,3 million pieces.
2. Personal computer is in 93,2% cases the device for access to Internet, mobile phone in 25,4% etc.
3. According to data of Ratel (Republic Telecommunication Agency) in Serbia is registered 199 internet providers who cover almost all larger inhabited places in the country.
4. This supercomputer performs 1 billiard operations in second.
5. In Germany there is a high conscience on the importance of data protection, as well as the strict legal penalties. Germany had demanded from Google to deliver them the hard discs with collected data, but this has not been done yet.
6. «Official Gazzete of the Republic of Serbia», no. 98/2006.
7. «Official Gazzete of the Republic of Serbia», no. 97/2008.
8. «Official Gazzete of the Republic of Serbia», no. 120/2004, 54/2007.
9. «Official Gazzete of the Republic of Serbia», no. 44/2003, 36/2006, 50/2009.
10. However, public telecommunications operator is obliged to provide for access and analysis of cited data to the authorized state bodies, in accordance with law. (Article 54. Law on telecommunications, „Official Gazette RS", no 44/2003, 36/2006, 50/2009.).
11. «Official Gazzete of the Republic of Serbia», no. 99/2006.
12. «Official Gazzete of the Republic of Serbia», no. 87/2006.
13. http://www.mtid.gov.rs/upload/documents/konsultacije/zek/ZEK%20nacrt%2022.10.pdf.
14. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
15. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML.
16. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.
17. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf.
18. According to the newest report Facebook has more than 300 millions active users, http://www.facebook.com/press/info.php?statistics.
19. http://blog.facebook.com/blog.php?post=7584397130.
20. http://www.dailymail.co.uk/sciencetech/article-1215470/Facebook-turns-controversial-advertising-Beacon.html.
21. http://www.cnn.com/2009/TECH/02/18/facebook.reversal/index.html.

22. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf.
23. In urban areas 46, 9% of inhabitants use Internet, and in rural areas only 22%.
24. Vuk Stefanović Karadžić (1787-1864) is the great Serbian reformer in the field of culture.
25. It is important for the domain to be shorter, to contain at least 2 letters. For example, Russia gave the proposal (as Russian Federation) for their domain.
26. Da operam, ne quid umquam invitus facias.

## References

[1] Riley T, *Privacy in the digital age*, Washington, 1997.

[2] Gross R. and Acquisti A, **„Information revelation and Privacy in Online Social Networks",** *ACM workshop on Privacy in the electronic society, Alexandria*, VA, USA, 2005.

[3] Young A. L and Quan-Hasse A, „Information revelation and internet privacy concerns on social network sites: a case study of face book, *Fourth international conference on Communities and technologies*, University Park, Pa, USA, 2009.

[4] http://www.cippic.ca/uploads/CIPPICFacebookComplaint-29May08.pdf

[5] http://www.priv.gc.ca/cf-dc/2009/2009-008-0716-e.pdf

[6] http://www.ifap.ru/library/book227.pdf

[7] www.datenschutz-berlin.de/attachments/.../WP-social-network-services.pdf

[8] http://www.priv.gc.ca/information/pub/sub-comp-200901-e.pdf

[9] http://webrzs.statserb.sr.gov.yu/axd/dokumenti/ict/2009/ICT2009s.zip

[10] Popović V, "*Zaštita privatnosti na Internetu kao jednom od servisa multimedijalnih komunikacija*", Magistarski rad, Saobraćajni fakultet, Beograd, 2004.

[11] Jovanović S, Drakulić M, Drakulić R, "Privatno - Javno? Sumrak privatnosti u eri društvenih mreža", *56. Naučno-stručni skup psihologa Srbije – Sabor psihologa*, Kopaonik, 2008.

# The use of genetic data in private insurance- problems and global perspectives

**Theodoros Trokanas**

## Introduction

The aim of this article is to present some of the problems arising from the use of genetic data in private insurance and to show how different legal systems around the globe have attempted to tackle those problems. After a short presentation of the American legal framework, the emphasis is placed on the European Continent, where the approaches adopted differ significantly. The last section of the article is devoted to the Greek legal environment in relation to this issue.

## Background information

The concept of "genetic information" is not something of a novelty. Traditionally, physicians have been using their patients' oral and written family medical histories, namely what other family members had suffered from or died of to make prognoses about their patients' possible illnesses[1]. However, the advancement of genetic engineering and the Bioinformatics Revolution, especially the successful completion of the Human Genome Project (HPG) in 2003, have broadened the scope of the notion "genetic information". Nowadays, information on the genetic code is often likened to "a coded probabilistic future diary"[2]. The significance attached to this kind of information is accentuated by the commercialization of genetic tests, which have become an integral feature of health care[3].

Broadly speaking, there are two categories of genetic tests: diagnostic and predictive[4]. Diagnostic tests are used to identify the presence or absence of a disease. Predictive genetic tests are divided into two sub-categories: predictive-presymptomatic genetic tests, which are used to predict if an individual will definitely have a disease in the future and predictive-predispositional tests, which are used to predict the risk of an individual developing a disease in the future. In general, both types of predictive genetic tests raise thorny ethical, social and legal issues. It has been reported that in 2009 genetic tests were available for 1.705 diseases, with 1419 being available for clinical diagnosis and 293 being available only for research[5].

## A subject for debate

Some months ago a highly interesting case surfaced in Australia[6]. An Australian insurance company named Nib Health Funds Ltd offered 5.000 of its customers reduced price genetic tests (from 1000 $ to 499 $) in collaboration with a Californian firm, Navigenics. However, in the small print of the insurance contract it was written that the results of these genetics tests are to be made available for consideration by the insurer should the latter wishes for it. This policy sparked off a heated debate, with a recurring question at the core: should genetic information be disclosed to insurers or not?

According to some theorists[7], the answer to the initial question should be "yes". It is argued that there is absolutely no reason for treating genetic information differently, insofar as it is not essentially different from other kinds of health information. In other words, it is not inherently more specific, predictive, sensitive or private than other kinds of health information. In addition, it is claimed that it is also extremely difficult to define what counts as genetic information, since it can be collected without anything which would be considered a genetic test (eg. is taking a family history a genetic test?).

I beg to differ on this view for a number of reasons. It is common knowledge that genetic tests do not yield conclusive results: firstly, because the exact mechanism of interrelationship between neighboring genes is not yet fully understood[8] and secondly, because the onset of an illness is attributed to complex interactions between genetic and environmental factors[9]. As a result, the reliability of genetic test is in most cases questionable[10]. For instance, genetic diagnosis may reveal susceptibility to a particular illness, but it cannot predict the probability of developing an illness, the exact time of its appearance or the severity of its symptoms[11]. What is more, the broad use of genetic testing raises concerns about the potential misuse or abuse of personal genetic data collected in the field of health insurance, which can lead to different forms of unfair genetic discrimination. From a purely philosophical perspective, it is morally wrong to penalize an individual for his or her bad luck in the genetic lottery, namely to make a person responsible for a genetic heritage, which is beyond his or her control[12]. Before examining what exactly the term "unfair genetic discrimination" implies, let me explain in parentheses some basic principles of health insurance.

## Statutory health insurance model vs. private health insurance model

There are two basic forms of health insurance: the statutory health insurance and the private health insurance. The first is based on the solidarity model or the no-

tion of social justice, whereas the second is based on the contract model. In reality, there is a world of difference between those two schemes. Inclusion in the statutory health insurance and the level of contributions payable are independent of the probability of a claim[13]. In fact, the balancing of solidarity between the healthy and the sick is a balancing of solidarity according to income level: the higher the income, the higher the contributions payable[14]. Another element of solidarity is that non-earning spouses and children are also covered usually with a minimal increase in contributions. The compulsory nature of this insurance scheme ensures that the entire group of insureds reflects the average distribution of "bad" and "good" health risks, insofar as no one can be excluded on the ground of poor health prospects and no one can dispense with insurance or negotiate lower contributions on the grounds of a good health prognosis[15].

On the other hand, private insurance is governed by the principle of risk equivalence[16]. To put it another way, the premium level for an insured is determined by the level of risk that he or she represents for the insurer[17]. Therefore, wherever a private health insurance contract is concluded, an *individual* risk assessment is made[18]. In practice, the insurer will assign a individual to an equal-risk group, which will include insureds of the same age, sex or similar medical histories[19]. A fundamental principle of the private model is that risks already existing or identifiable at the time of conclusion of the contract are not borne jointly by the insureds[20]. As a result, anyone who is already ill or old at the time of the conclusion of a contract pays a higher premium. An insurer may even exclude a given risk from coverage or decline to conclude a contract at all[21]. Finally, another characteristic of private insurance is that a separate contract must be concluded for each insured person (spouse, children).

In Europe, taking out private health insurance is still voluntary or at least subsidiary to the statutory health insurance. On the contrary, it is well-known that private health insurance is the norm in the USA.

## Potential manifestations of genetic discrimination in the field of health insurance

Genetic discrimination in the field of health insurance can take different forms, such as refusal to insure an individual altogether, imposition of higher premiums, refusal to provide coverage for a particular treatment, or refusal to compensate. These practices are based on a misinterpretation of genetic test results, and in most cases on equating a genetic predisposition to a "preexisting condition".

Another -more insidious- form of genetic discrimination can arise from the proliferation of a practice according to which a prospective insured voluntarily submits favorable to himself results of genetic tests in order to negotiate lower

premiums[22]. This practice would mean that everyone failing to supply such results would automatically be considered a suspect, whether concealing a genetic predisposition or just being unaware of it. Obviously, a rational insurer would respond by increasing premiums indiscretely for both categories, forcing in that way people who may not wish to take a genetic test to submit to it[23]. This is why the contention that voluntary disclosure of favorable genetic results should be legally frustrated[24] is something which I align myself with.

Besides, disclosure of an individual's genetic information can limit access to insurance for other family members. For example, if an insurance company becomes aware of specific test results, it may refuse to insure children who may have inherited their father's predisposition to a disease.

Let me close this unit with the following remark: it is startling to learn that genetic discrimination can potentially affect every human being, because every human carries 5 to 7 fatal recessive genes and up to 30 predispositions to various disorders[25].

## Multi-faceted impact of genetic knowledge

In the first place, the very same knowledge of a genetic predisposition will impose a heavy psychological burden on an individual, especially if the disease concerned is neither avoidable nor curable. This can seriously disrupt his or her normal course of life or come as a shattering blow to his or her self-esteem and self-image. On a social level, individuals with a genetic proclivity may also face stigmatization or even exclusion. As a matter of fact, it is argued that genetic research and testing can reinforce racial, ethnic or gender stereotypes, insofar genes define one's race, ethnic background, sex and sexual orientation[26].

Apart from the knowledge itself, even the fear of genetic discrimination based on genetic testing can affect the health of a person and his or her family environment. The fear of genetic discrimination may prevent individuals from undergoing tests, the results of which could be used for beneficial purposes. Undoubtedly, being aware of a predisposition to a disease or of a possible adverse drug reaction and taking the necessary preventive steps is in the best interests of an individual[27]. Likewise, genetic knowledge can help individuals or their family members make informed choices about their reproduction or career (e.g. avoidance of certain hazard-prone jobs)[28]. Furthermore, another concern often expressed is that some individuals may even withhold genetic information from their own physicians, putting their lives in a higher health risk[29]. On the other hand, the reluctance of an individual to undergo genetic tests can indirectly affect other family members[30]. Since some genetic illnesses are hereditary in na-

ture, early detection on an individual might be the key to protecting the health of his or her family circle as well.

Additionally, it is considered that the fear of genetic discrimination hinders clinical research[31]. This is because many people refuse to participate in clinical studies for fear of having their genetic data used against them by insurers or employers. Consequently, researchers lose valuable resources which in the long run could help create more efficient, cost-effective genetic tests and most importantly could lead to cures for numerous diseases.

Lastly, it is the economic impact of genetic test avoidance that is underlined[32]. Refusal to undergo genetic testing, which entails late detection of illnesses, can increase the financial strains on patients, their families and society as a whole, the health care system naturally included. On the contrary, the use of genetic tests could allow doctors to prescribe more economical preventive treatments instead of expensive remedial ones.

## Legal aspects of genetic discrimination

The collection of genetic data by insurers has provoked severe criticism, for it poses a threat for the private sphere of the prospective insured. In other words, it constitutes an infringement of the fundamental right to self-determination and in particular the right to ignorance[33]. Here, the right of ignorance should be conceived as a protection of an individual against having genetic information forced upon him or her. It is also stressed that the right to ignorance is violated, even if the insurer, with the consent of the former, conceals the genetic information collected, since conclusions can be drawn from the content of an insurance contract itself. For instance, an unusually high premium would make an insured realize that he or she represents an above-average health risk.

## Regulatory frameworks for genetic data use in health insurance

### *The United States of America model*

Following a 13 year debate in Congress (1995-2008), the Genetic Information Non-discrimination Act (or GINA for short) was signed into law by ex-President Bush on 21 May 2008. This Act has been hailed as the "first major Civil Rights Bill of the century"[34], as it creates a national baseline for safeguards against discrimination[35].

Prior to GINA the only federal legislation which addressed genetic discrimination was the Health Insurance Portability and Accountability Act (or HIPPA for short) of 1996. HIPPA set forth that genetic information cannot be considered a "*preexisting condition*" in the absence of a diagnosis of the condition related to

such information[36]. However, the problem with HIPPA was that it applied only to group health plans, thus not covering the individual insurance market. This gap was filled with GINA.

GINA addresses genetic discrimination and the privacy of genetic information in two settings, health insurance and employment. Its main objective was to allay public fears about possible discriminations in both these contexts. Title I of the Act covers the use of genetic information in health insurance and takes effect on 1 January 2010.

GINA's definitions of the term "genetic information" encompass a wide variety of genetic tests as well as a broad range of family medical records[37]. The term "genetic information" means, with respect to any individual, information about (i) such individual's genetic tests, (ii) the genetic tests of family members of such individual and (iii) the manifestation of a disease or disorder in family members of such individual[38]. The term "family member" embraces up to fourth-degree relatives[39]. In addition, any reference to genetic information concerning an individual or family member of an individual who is a pregnant woman includes genetic information of any fetus carried by such pregnant woman; and with respect to an individual or family member utilizing an assisted reproductive technology includes genetic information of any embryo legally held by the individual or family member[40].

The term *«genetic test»* means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes[41]. Nevertheless, it does *not* mean (i) an analysis of proteins or metabolites that does not detect genotypes, mutations, or chromosomal changes; or (ii) an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition that could reasonably be detected by a health care professional with appropriate training and expertise in the field of medicine involved[42].

Cornerstone of GINA is the limitation imposed to insurers on requesting or requiring that an individual -or his or her family member- undergo genetic testing[43]. Nonetheless, it is explained that this rule is not intended to discourage a physician from recommending a genetic test to be used for therapeutic or preventative ends[44].

Another contribution of GINA is the equation of genetic information with health information under the declaration that "Genetic information shall be treated as health information"[45]. This means that genetic information enjoys the same level of protection as regular health information. In this sense, the use or disclosure of protected health information that is genetic information for "underwriting pur-

poses" is not a permitted use or disclosure[46]. The term "underwriting purposes" with respect to a group health plan, health insurance coverage, or a medicare supplemental policy means: (A) rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy; (B) the computation of premium or contribution amounts under the plan, coverage, or policy; (C) the application of any pre-existing condition exclusion under the plan, coverage, or policy; and (D) other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits[47].

Finally, GINA claims credit for prohibiting health discrimination on the basis of genetic information. In particular, it stipulates that "a health insurance issuer offering health insurance coverage in the individual market (a) may not establish rules for the eligibility (including continued eligibility) of any individual to enroll in individual health insurance coverage based on genetic information[48]; (b) shall not adjust premium or contribution amounts for an individual on the basis of genetic information concerning the individual or a family member of the individual[49]; (c) may not, on the basis of genetic information, impose any preexisting condition exclusion[50]".

### *The stance of the European Union*

Very early the European Parliament adopted the Resolution of 16 March 1989 on the ethical and legal problems of genetic engineering which considers that "insurance companies have no right to demand that genetic testing be carried out before or after the conclusion of an insurance contract nor to demand to be informed of the results of any such tests which have already been carried out and that genetic analysis should not be made a requirement for the conclusion of an insurance contract". Some years later the Council of Europe approved the Recommendation No R. (92) 3 on genetic testing and screening for health care purposes which was adopted by the Committee of Ministers on 10/02/1992. This text proposes a set of principles, among which highlights principle 7 with the following content: "insurers should not have the right to require genetic testing or to enquire about results of previously performed tests, as a pre-condition for the conclusion or modification of an insurance contract". It should be noted, though, that both these texts are not legally binding.

On the contrary, a legally binding text one could turn to is the Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine of 04/04/1997 (or Oviedo Convention for short). The Oviedo Convention includes three general provisions of critical importance to the matter in question.

Firstly, according to article 11 of the Oviedo Convention "Any form of discrimination against a person on grounds of his or her genetic heritage is prohibited"[51]. Greek theorists[52] have suggested that the requirement for undergoing genetic tests imposed by private insurance companies to prospective insureds before the conclusion or for the continuation of a contract constitutes an unfair discrimination, for it basically deprives the (prospective) insureds of their right to private insurance.

Secondly, the article 12 of the Oviedo Convention lays down that "Tests which are predictive of genetic diseases or which serve either to identify the subject as a carrier of a gene responsible for a disease or to detect a genetic predisposition or susceptibility to a disease may be performed only for health purposes or for scientific research linked to health purposes, and subject to appropriate genetic counselling". The Explanatory Report accompanying the Oviedo Convention elucidates the article by stating that there should be a distinction between health care purposes for the benefit of the individual and health care purposes which cater to third parties' interests and may be commercial[53]. In fact, in the same Report it is made clear that it is forbidden to carry out predictive genetic tests for reasons other than health or health-related research, even with the assent of the person concerned[54]. This prohibition is grounded in the fact that "it entails a disproportionate interference in the rights of the individual to privacy"[55]. The Explanatory Report reaches the conclusion that "an insurance company will not be entitled to subject the conclusion or modification of an insurance policy to the holding of a predictive genetic test. Nor will it be able to refuse the conclusion or modification of such a policy on the ground that the applicant has not submitted to a test, as the conclusion of a policy cannot reasonably be made conditional on the performance of an illegal act"[56].

Thirdly, the Oviedo Convention in article 10 §2 establishes the "right not to know" under the following formulation: "Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed". Greek theorists[57] have argued that the requirement for undergoing genetic tests imposed by private insurance companies to prospective insureds violates their right to ignorance of their genetic data.

### *The stance of individual European countries*

In this section of the article will be outlined the attempts made in some European countries to handle this issue[58].

### The British model

Even though in Great Britain there is no legal regulation of the subject, the country sets a very good example of self-regulation. In 2001 The Association of Brit-

ish Insurers (ABI)[59] and the Government signed a policy agreement entitled "Concordat and Moratorium on Genetics and Insurance", concerning the use of genetic test results in insurance for underwriting purposes[60]. The text sets conditions under which genetic tests may or may not be used. The Concordat builds on the voluntary "ABI Code of Practice for Genetic Tests", which was first elaborated in 1997 and whose current edition came into effect on 13/06/2008. In 2008 the ABI publicly announced its intention to extend the force of the agreement to 2014[61].

As it has already been mentioned, there are two broad categories of genetic tests: predictive genetic tests, which are taken prior to the appearance of any symptoms of the condition in question and diagnostic genetic tests, which are taken to confirm a diagnosis based on existing symptoms[62]. The scope of the Concordat is narrowed to predictive genetic tests (i.e. the small number of tests used to predict future illnesses) and not to the majority of genetic tests which confirm diagnoses of ill health and inform treatments[63]; much less, the Concordat does not concern non-genetic medical tests (blood or urine tests for cholesterol, prostate cancer, liver function or diabetes)[64]. Therefore, insurers are permitted to seek, with customer's consent, access to certain family medical history, diagnostic genetic test results and to reports from General Physicians (GPs)[65].

A crucial contribution of the Concordat is the assignment of the evaluation of the results of predictive genetic tests to an independent advisory body, the Genetic and Insurance Committee (or GAIC for short)[66], in an attempt to prevent misunderstanding or overestimation of genetic information on the part of insurers.

The basic principle to which both texts adhere is the principle of non-discrimination based on genetic information. The Concordat[67] declares that "insurers should not treat customers who have an adverse predictive test result less favourably than others without justification". In a converse formulation, the ABI Code of Practice states that "insurers may only take into account adverse results of those predictive genetic tests that the government's advisory body GAIC has decided are technically, clinically and actuarially relevant"[68]. The same Code of Practice specifies that there must be no increase in the premium or worsening in the terms an insurer offers, arising from such a test, unless there is a similar GAIC decision[69]. Furthermore, the Code means to discourage an indirect form of genetic discrimination: insurers must not offer individual lower than standard premiums on the basis of their predictive test results[70]. Finally, according to the same Code, a predictive genetic test result declared by an applicant may not be linked to, or taken into account during the assessment of an application for insurance from another person[71].

In practice, the most effective way to ensure the implementation of the principal of non-discrimination is by not allowing genetic tests to become a prerequisite for the conclusion of an insurance contract. This is why both the Concordat and the Code of Practice provide that "applicants will not be asked to, nor be put under any pressure to, undergo a predictive genetic test in order to obtain insurance"[72]. This guiding principle is further strengthened with the suspension of the principal of disclosure. In other words, applicants are under no obligation to disclose either their own or another person's (eg. a blood relative's) genetic test results (including those acquired as a part of clinical research)[73], regardless of the time when these tests were taken (before or after the Concordat policy has come into force)[74].

However, there are some exceptions which lead to the reapplication of the rule of disclosure. Insurers are permitted to use information from predictive genetic test if the following conditions are met: (a) if the predictive test is approved by the government's GAIC and (b) if the application for insurance is above the financial limits set out in the moratorium[75]. As far as the first condition is concerned, to date the GAIC has only approved the Huntington's disease genetic test. As far as the second condition is concerned, according to the terms of the Moratorium, customers will not be required to disclose the results of predictive genetic tests for policies up to £500.000 of life insurance, or £300.000 for critical illness insurance, or paying annual benefits of £30.000 for income protection insurance[76].

Finally, an applicant is allowed to disclose a favourable (negative) predictive genetic test result in order to override his or her known medical or family history, i.e. to reduce the impact of loading or to nullify a potential exclusion which would otherwise have applied[77].

## The French model

The French Civil Code in article 16-13[78] includes a general clause prohibiting any form of discrimination based on genetic characteristics. Any violation of the above principle is liable to penal sanctions[79]. More specifically, the article L1141-1 of the French Code of Public Health prohibits insurance companies from taking into consideration genetic test results of a person, even if these results are supplied with his or her consent. Additionally, insurance companies cannot require that a person undergo a genetic test either before the conclusion of an insurance contract or during its duration. It is obvious that in the French legal system there exists an absolute ban on the use of genetic data by insurers[80].

## The Swiss model

On 08/10/2004 Switzerland passed a federal law on human genetic testing (Loi fédérale sur l'analyse génétique humaine - LAGH) which came into effect on

01/04/2007. This law uses the term "pre-symptomatic genetic tests" to refer to genetic tests which aim to detect a predisposition to an illness before the appearance of clinical symptoms, with the exclusion of tests which aim only to confirm the effects of a potential treatment[81].

The Swiss law also includes a general clause of non-discrimination because of genetic inheritance[82]. Moreover, it establishes "the right not to be informed" about one's genetic inheritance, with a view to protecting individual autonomy[83]. This right to self-determination with regard to undergoing genetic tests is elaborated on in article 18 of the law.

As far as the use of genetic tests in the domain of insurance is concerned, the Swiss law provides that an insurer may not require prior to the establishment of an insurance relation a pre-symptomatic or prenatal genetic test[84]. However, this fundamental principle is subject to exceptions. According to article 26 an insurer can require results for pre-symptomatic genetic tests already taken for policies more than 400.000 SFR or paying annual benefits of more than 40.000 SFR for illness insurance[85].

It is manifest that the Swiss legal system does not enforce an absolute ban on the use of genetic data by insurance companies, so that a partial disclosure of such information can occur.

## The German model

The German Parliament voted on 24/04/2009 a law on human genetic tests (Gendiagnostikgesetz-GenDG) which came into force in July 2009[86]. In §6 (1) of the law there is a general prohibition on discriminating persons because of their own or the genetic qualities of a relative, as well as because of their or a relative's decision to undergo or not a genetic test or because of the result of such a test. In §18 (1) the German law disposes that an insurer either before or after the conclusion of an insurance contract may not require that a person undergo genetic tests or require that he be informed of the results of genetic tests carried out or such results receive or use. However, this does not apply to high-value policies, i.e. if the payout is more than 300.000 € or there is an annual pension payment of more than 30.000 €.

## The Italian policy

Italy belongs to the group of countries which have not yet enacted a specific law about the issue in question. However, a group of scientists working under the auspices of both the National Bioethics Committee and the National Committee for Biosecurity, Biotechnology and Life Sciences have issued a Recommendation in May 2008 entitled "*Genetic Testing and Insurance*" as a contribution of the coun-

try to the widespread European debate which is already in progress. The Italian working group is in favor of a moratorium regime until the end of the European debate. In addition, it suggests that insurance companies adhere to a self-regulation procedure and commit themselves to protecting personal data. Finally, the same group insists that insurance companies should not demand that their clients undergo genetic testing in order to obtain insurance. Nevertheless, the Recommendation includes two exceptions to the above rule: the first one is that insurance companies can request and have access to *diagnostic* genetic test results taken previously by clients for any insured amount; the second exception is that if the insured amount exceeds a certain limit, insurance companies can request and have access to *presymptomatic* genetic tests results previously taken by clients.

## The Greek policy

In Greece there is no specific regulation on the use of genetic data in private insurance. For this reason, one should turn to the general provisions of the Oviedo Convention, which has been ratified with Law 2619/1998 and came into force on 01/12/1999. Specifically, the aforementioned articles 10, 11 and 12 of the Convention could prove applicable here. The obvious disadvantage, though, is that having the form of general clauses, all three articles do not suffice to solve concrete problems.

As for non-binding texts, The National Commission of Bioethics (N.C.B) officially addressed the issue twice: the first time was with the "Recommendation on the collection and use of genetic data" issued on 16/09/2002 and the second time was with the "Opinion on the use of genetic data on private insurance" issued on 11/01/2008[87].

In its first Recommendation, the N.C.B draws a distinction between public social security and private insurance. Specifically, it deems the disclosure of genetic information to public security funds unacceptable, even with the consent of the (prospective) insured, insofar as social security is a public good and thus should be made available to everyone without discrimination. As far as private insurance is concerned, any disclosure of genetic data is also unacceptable if the (prospective) insured does not enjoy public social security coverage[88]. Finally, when private insurance is subsidiary to social security, disclosure is permitted, on condition that the (prospective) insured has granted his or her consent.

In its second Opinion the N.C.B. delves deeply into the matter. To begin with, it perceives the matter as a case of conflict between two constitutionally safeguarded rights: the protection of personality of the insureds and the economic freedom (freedom of contract) of insurers. Disclosure of genetic data touches the core of personality, since it constitutes sensitive personal data. On the other hand, bar-

ring insurers from access to genetic information may seem unfair, since it exposes them to risks they ignore. The N.C.B. concludes that the protection of the insured outweighs the economic freedom of the insurers, considers that insurance market cannot be significantly harmed by the prohibition of genetic discrimination in risk calculation. However, the N.C.B proposes safeguarding the legitimate interests of the insurers, and especially in the direction of eliminating the risk of willful deception. In the same Opinion the N.B.C. underlines the need for regulation on this field, taking into account the weaknesses of the Greek social security system in conjunction with the steady expansion of the private life and health insurance market. Until the elaboration of a relative legislation on the matter, the N.C.B thinks it is expedient to adopt a moratorium with a reasonable duration.

## Conclusion

The presentation made in this article does not pretend to exhaust the issue of genetic data use in private health insurance. Instead, it intends to give the reader an overview of the emerging problems in this domain and the divergent paths followed to cope with them. The situation in the European space is characterized by a regulatory disparity: from the absence of any regulation or the encouragement of self-regulation initiatives to the introduction of rigorous legal regulation on the subject. Generally, all efforts made aimed at protecting genetic privacy and preventing genetic discrimination. It is noteworthy, though, that in those countries where specific legislation has been voted, the main criticism leveled is that this legislation has exceptions and loopholes. It is forecast that the issue will pose itself more imperatively in many European member-states, where a gradual shift from the statutory insurance model to the private insurance model is being monitored. This tendency is basically due to the decline of the notion of welfare state and the decrease of social security benefits in European countries with national deficits, which entail budget cuts. As far as Greece is concerned, the question is whether the existing legal framework suffices. It is my firm conviction that we are in need of more specific legislation modeled on the legislative frameworks set in USA and other European countries.

## Endnotes

1. Payne P., Genetic Information Nondiscrimination Act of 2008: The federal answer for Genetic Discrimination, Journal of Health Biomedical Law, 2009, p. 35. On the nature of genetic information see also Bottis M., Comment on a view Favoring ignorance of genetic information: Confidentiality, autonomy and the right not to know, EJHL 2000, 7 (2), pp. 173-183.
2. Weeden J.-L., Genetic liberty, genetic property: protecting genetic information, Ave Maria Law Review, Summer 2006, p. 618.

3. Ziskid S., The Genetic Information Nondiscrimination Act: A new look at an old problem, Rutgers Computer and Technology Law Journal, 2009, p. 168.
4. Nuffort L.-E., The Genetic Information Nondiscrimination Act of 2008: raising a shield to genetic discrimination in employment and health insurance, Health Lawyer, June 2009, p. 5.
5. Ibidem.
6. "Cut-price DNA test could prove costly, experts warn", 22 February 2010 on www.bionews.org.uk.
7. Holm S., Should genetic information be disclosed to insurers? YES, BMJ, 9 June 2007, vol.334, p. 1196.
8. O'Hara S., The use of genetic testing in the health insurance industry: the creation of a 'biologic underclass', Southwestern University Law Review, 1993, p. 1219.
9. Ziskid S., op. cit., p. 176. O'Hara S., op. cit., p. 1218.
10. Katz G. / Schweitzer S., Implications of genetic testing for health policy, Yale Journal of Helath Policy, Law and Ethics, Winter 2010, p. 99.
11. Ziskid S., op. cit., p. 176. O'HARA S., op. cit., p. 1212 and 1215-1216.
12. Ziskid S., op. cit., p. 175.
13. Opinion of Nationaler Ethikrat Predictive Health Information in the conclusion of insurance contracts, 2007, under E, 1.1.
14. Ibidem, under E, 1.1.
15. Ibidem, under E, 1.1.
16. Ibidem, under B, 1.
17. Ibidem. under B, 1.
18. Ibidem, under B, 2.1.
19. Ibidem, under B, 1.
20. Ibidem, under E, 1.2.
21. Ibidem, under E, 1.2.
22. Ibidem, under F, 4.6.
23. Ziskid S., op. cit., p. 197-198.
24. Ziskid S., op. cit., p. 199.
25. Formas-Norris C., The Genetic Information Non-Discrimination Act of 2008: History, Successes and future considerations, Comment, University of Maryland Law Journal of Race, Religion, Gender and Class, Spring 2007, under I.
26. Formas-Norris C., op. cit., under II, D. It is reminded by the same author that in the 1970s some states in the USA had instituted mandatory sickle cell anemia screening programs for African-Americans, on the grounds that individuals with this disease carried a heightened risk form some workplace toxins (Formas-Norris C., op. cit., footnote 72).
27. Formas-Norris C., op. cit., under II, B.
28. Ziskid S., op. cit., p. 170. On data protection and electronic health records generally see Bottis M., Confidentiality and data protection in electronic health records, in Mitrou L., Gritzalis D. and Labrinoudakis K. and Katsikas S. (eds.), Privacy Protection - Technologies of Computer

Science and Communications, Technical and Legal Matters, Papasotiriou 2010, pp. 567-580 (in Greek).

29. Lee J., The first civil rights Act of the 21st century: Genetic Information Nondiscrimination Act of 2008, A Journal of Law and Policy for the Information Society, Winter 2008-2009, p. 787.
30. Lee J., op. cit., p. 788.
31. Formas-Norris C., op. cit., under II, C. LEE J., op. cit., p. 788.
32. Lee J., op. cit., p. 788.
33. Opinion of Nationaler Ethikrat Predictive Health Information in the conclusion of insurance contracts, under D, 3.
34. Abiola S., The Genetic Information NonDiscrimination Act of 2008: "First major civil rights Bill of the century" bars misuse of genetic test results, Journal of Law, Medicine and Ethics, Winter 2008, p. 856.
35. Ibidem.
36. Sec. 2701, (b), (1), (B). What is meant by that is that if an individual's test reveals a gene mutation linked to breast cancer (BRCA1 or BRCA2), this piece of information cannot be treated as a preexisting condition in the absence of a diagnosis of breast cancer.
37. Ziskid S., op. cit., p. 179.
38. Gina, Sec. 102 (f), (16), (A).
39. Gina, Sec.102 (f), (15).
40. Gina, Sec. 102 (f), (1-2).
41. Gina, Sec. 102 (f), (17), (A).
42. Gina, Sec. 102 (f), (17), (B).
43. "A health insurance issuer offering health insurance coverage in the individual market shall not request or require an individual or a family member of such individual to undergo a genetic test" [GINA, Sec. 2753, (d), (1)].
44. "However, this shall not be construed to limit the authority of a health care professional who is providing health care services to an individual to request that such individual undergo a genetic test" [GINA, Sec. 2753, (d), (2)].
45. Gina, Sec. 1180 (a), (1).
46. Gina, Sec. 1180 (a), (2).
47. Gina, Sec. 1180 (b), (4).
48. Gina, Sec. 2753 (a), (1). However, this shall not be construed to preclude a health insurance issuer from establishing rules for eligibility for an individual to enroll in individual health insurance coverage based on the manifestation of a disease or disorder in that individual, or in a family member of such individual where such family member is covered under the policy that covers such individual [GINA, Sec. 2753 (a), (2)].
49. Gina, Sec. 2753 (b), (1). However, this shall not be construed to preclude a health insurance issuer from adjusting premium or contribution amounts for an individual on the basis of a manifestation of a disease or disorder in that individual, or in a family member of such individual where such family member is covered under the policy that covers such individual. In such

case, the manifestation of a disease or disorder in one individual cannot also be used as genetic information about other individuals covered under the policy issued to such individual and to further increase premiums or contribution amounts [GINA, Sec. 2753 (b), (2)].

50. Gina, Sec. 2753 (c), (1). However, this shall not be construed to preclude a health insurance issuer from imposing any preexisting condition exclusion for an individual with respect to health insurance coverage on the basis of a manifestation of a disease or disorder in that individual [GINA, Sec. 2753 (c), (2)].

51. This general clause of non-discrimination in the Oviedo Convention harmonizes with four other non-binding (both european and international) texts: (1) the Additional Protocol to the Convention on Human Rights and Biomedicine concerning Genetic Testing for Health Purposes of 27/11/1998, where it is declared that "Any form of discrimination against a person, either as an individual or as a member of a group on grounds of his or her genetic heritage is prohibited" (article 4 §1) as well as that "Appropriate measures shall be taken in order to prevent stigmatization of persons or groups in relation to genetic characteristics" (article 4 §2). This Protocol has not been signed by the majority of European countries yet, including Greece; (2) the Charter of Fundamental Rights of the European Union elaborated on 17/12/2002 in article 21 §1 affirms that "Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited"; (3) the Universal Declaration on Human Genome and Human Rights adopted by the United Nations on 11/11/1997, where article 2 (a) in a positive formulation proclaims that "Everyone has a right to respect for their dignity and for their rights regardless of their genetic characteristics", whereas article 6 in a negative formulation proclaims that "No one shall be subjected to discrimination based on genetic characteristics that is intended to infringe or has the effect of infringing human rights, fundamental freedoms and human dignity"; (4) the International Declaration on Human Genetic Data drawn up by UNESCO adopted on 16/10/2003, where Article 7 (a) proclaims: "Every effort should be made to ensure that human genetic data and human proteomic data are not used for purposes that discriminate in a way that is intended to infringe, or has the effect of infringing human rights, fundamental freedoms or human dignity of an individual or for purposes that lead to the stigmatization of an individual, a family, a group or communities".

52. Frangoudaki H., The legal treatment of applications of biogenetics –especially in private law sector, An t. N. Sakkoulas Publishers, Athens-Komotini, 2008, p. 357.

53. Explanatory Report to the Oviedo Convention, under 84.

54. Ibidem, under 85.

55. Ibidem, under 86.

56. Ibidem, under 86.

57. Greek National Commission of Bioethics, REPORT on genetic data in private insurance, authored by T. Vidalis, A.L. Hager-Theodorides in collaboration wih G. Maniatis, available on www.bioethics.gr.

58. For a comprehensive presentation see the official document of the European Commission entitled "Survey on national legislation and activities in the field of genetic testing in EU Member States" of 1 May 2005.

59. The ABI is the trade association for Britain's insurance industry with more than 400 member companies which provide over 97% of the insurance business in the UK.
60. In Finland, an official agreement states that genetic information is not used for health insurance purposes.
61. Abi News Release of 13 June 2008, available on www.abi.org.uk. See also "UK insurance moratorium on use of genetic data extended until 2014", appeared on 16 June 2008 on www.bionews.org.uk.
62. Abi Code of Practice for Genetic Tests, June 2008, under 2.1.
63. Concordat and Moratorium on Genetics and Insurance, March 2005, under 4.
64. Ibidem, under 12.
65. Ibidem, under 16 (vi).
66. Ibidem, under 11: "The technical, clinical and actuarial relevance of predictive genetic test results should be subject to independent oversight through GAIC".
67. Ibidem, under 11.
68. Abi Code of Practice for Genetic Tests, under 6.2.
69. Ibidem, under 6.3.
70. Ibidem, under 6.5.
71. Ibidem, under 10.3.
72. Concordat and Moratorium on Genetics and Insurance, under 16 (i). ABI Code of Practice for Genetic Tests, under 6.1.
73. Abi Code of Practice for Genetic Tests, under 9.1 and 10.4.
74. Concordat and Moratorium on Genetics and Insurance, under 16 (v).
75. Abi Code of Practice for Genetic Tests, under 10, 1 a and b.
76. Concordat and Moratorium on Genetics and Insurance, under 20 (i). It is reported that more than 97% of policies issued in 2004 were below these limits in each category.
77. Abi Code of Practice for Genetic Tests, June 2008, under 6.5, 10.1 b and 10.2.
78. Article 16-13 French Civil Code: "No one may be discriminated against on the basis of his genetic features" (official translation from Legifrance).
79. Articles 225-1 to 225-4 French Penal Code.
80. In Belgium, a Royal Decree prohibits the use of genetic information for private insurance.
81. Article 3 b Loi fédérale sur l'analyse génétique humaine (LAGH).
82. Article 4 LAGH: "Nul ne doit être discriminé en raison de son patrimoine génétique".
83. Article 6 LAGH: "Toute personne peut refuser de prendre connaissance d'informations relatives à son patrimoine génétique".
84. Article 26 LAGH.
85. Article 27 1 d-e LAGH.
86. In Austria, a general ban on using genetic tests and genetic information in health insurance was introduced with the Gentechnology Act of 1994 (Gentechnikgesetz, BGBl. Nr. 510/1994).

87. Both texts are available on the official site of the National Commission of Bioethics www.bioethics.gr.

88. For the same opinion see also Mallios E., Genetic Tests and Law, Sakkoulas Publications, Athens-Thessaloniki, 2004, p. 93.

# User-created content v. Copyright: Two worlds collide?

**Thanos Tsingos**

## Introduction

In the dawn of the 21st century the whole world is amazed by the spectacular development of new communication technologies that play the most crucial role to the configuration and function of the so-called "information society". The daily life is, nowadays, substantially affected and by far determined by the very fast transmission of information. The Internet is, undoubtedly, a unique means of distance communication and the cornerstone of the today's communication technologies.

However, new internet–based technologies (collectively called as "Web 2.0 technologies) go beyond of serving a mere communication goal and provide users with the technical ability to produce content for various reasons (commentary, criticism, entertainment, etc) and then display it publicly on the web. Such content (well known as "user-created content") is usually based on existing works and is subsequently developed to a new work by means of a personal contribution.

In this context, the most important issue that seems to arise is whether users infringe the owners' exclusive right(s) both in the production process and at the time the new work is displayed publicly on the web, just in case that the already existing work is protected by copyright. If the answer to the previous question is affirmative, one has to further examine whether Intellectual Property Laws provide for a possible limitation or exemption to the owners' exclusive rights for the sake of user – created content.

So, the paper seeks to offer a wider discussion on the legal framework that is relevant to the previous questions and extract the most recent developments in this particular area of law. The analysis will begin in Part I by presenting the background of the "user created content" as a phenomenon in the Information Society. In this part, the author explains the use of "Web 2.0" technologies, its interaction with the web hosting services and the new role of the creative user in the information society.

In part II, the author will focus on the creative process. The central issue to be analyzed is how the copyright law (especially in the EU legal framework) perceives the acts of transforming an already existing copyrighted work into a new one and

displaying such new works on the Internet. For the purpose of the analysis the author considers the existing works as already protected by copyright.

Part III is dedicated to the discussion of whether a possible exemption or limitation to the owners' exclusive right(s) is provided for by the Intellectual Property Laws. In this interesting part, we first mention the relevant provisions of the Berne Convention, as envisaged by the TRIPS Agreement and the other WTO Treaties, incorporating the well known "three-step test". After analyzing the test in the light of the relevant WTO Panel Reports, the WIPO official documents and the academic literature, we then turn our discussion into the European Community level. In this context, we examine the provisions of Directive 2001/29/EC "on the harmonization of certain aspects of copyright and related rights in the information society" enhanced by the EU official documents, which also reflect the recent debate about the "creative content on line".

The final Part is dedicated to the conclusions of the analysis that took place above. The author attempts to assess the findings of the analysis in a critical way, thereby addressing the developments of law and presenting the problems arising out of the application of the existing Legal framework. The proposed paper purports to prefigure the future implications and the challenges of the existing regulatory framework.

## User created content and the information society

The end of the earlier century is spotted by the emergence of the World Wide Web, a technological invention that would change the human kind's daily life for ever. This is often known as the "Web 1.0" phenomenon. The Internet, its key – tool was designed to facilitate world's distance communication thereby reducing time, money and human activity.

At first glance, that did not seem to be such an outstanding innovation, simply because it was difficult – in the common sense - for the advantages of this new technology to be immediately understood by the vast majority of people. The devolvement from the analogue to the digital world needed some time to be completed. It was just between the late of the earlier and the beginning of the 21st century, when the "Web 2.0" phenomenon invaded and the whole world welcomed the Information Age once for all. This phenomenon is largely responsible for the formulation and function of the so called Information Society, that is, "…a society in which the creation, distribution, diffusion, use, integration and manipulation of information is a significant economic, political, and cultural activity" [Wikipedia].

Web 2.0 technologies could be successfully determined as "...web applications that facilitate interactive information sharing, interoperability, user-centered design and collaboration on the World Wide Web." In other words, Web 2.0 applications allow its end-users to interact with each other as contributors to a website's content, in contrast to websites where users are limited to the passive viewing of information that is provided to them. Search engines (e.g. Google and Yahoo), blogs, wikis, distribution platforms (eg. You-Tube and Flickr), social networks (e.g. MySpace, Frendster, Facebook) and virtual worlds (e.g. Second Life) are just examples from the Web 2.0 inexhaustible technology list.

Web 2.0 applications are associated with the web – hosting services. A web hosting service, in particular, is a type of Internet hosting services which is constructed to perform a double task: In the first place, it allows individuals and organizations to provide their own website accessible via the WWW, while in a second place, third parties are able to access these websites and exercise additional capabilities of uploading content in this particular part of the cyberspace [I. Igglezakis, 2002].

In the abovementioned technology context, one should consider the much intended purpose for which those technologies are designed. Indeed, all of these web-based 2.0 applications present a unique and common characteristic, that of providing end users with the technical ability to create content and then make it available online. Users are nowadays able to upload content on – line, which is either of their own exclusive creation (e.g. post comments, book reviews or even upload their articles and other artistic works) or constitutes an already existing work (e.g. post songs, films or portions thereof on distribution platforms).

But between these two categories of content, one may identify the possibility of uploading content that derives from the combination of an already existing work along with a personal contribution. In that particular in-between category one may identify three possible activities, that is: mashing up (taking a digital media file containing any or all of text, graphics, audio, video and animation drawn from pre-existing sources to create a new derivative work), sampling (taking a portion or sample of one sound recording and reusing it as an instrument or a different sound recording of a song) and remixing (taking samples from pre-existing materials to combine them into new forms according to personal taste) [Hemmungs Wirten, 2009]. Mash – ups, as songs composed entirely of pieces of pre-existing sound recordings, can be seen as "a subset" of sampling, while the scope of remixes is much broader than mash-ups, since the former can involve art, literature, or film in addition to music, and need not be composed entirely of pieces of pre-existing expression [Reynolds, 2009].

In any case, all of these types of "artistic appropriation" constitute a newly introduced phenomenon of the so - called "user – created content (UCC)" or "user

– generated content (UGC)" or "consumer-generated media" (CGM). This concept is associated with the new web 2.0 technologies and actually implies various kinds of media content, publicly available, produced by end-users for various reasons (commentary, criticism, entertainment, etc), when acting outside their profession or business [G. Carlisle - J. Scerri, 2007, p. 2]. In other words, one may identify such content in the cyberspace, if three conditions are to be cumulatively met: i) content made publicly available over the Internet ii) which reflects a certain amount of creative effort, and iii) which is created outside of professional routines and practices [OECD, 2007].

Appropriation art is not a new concept – the practice was prominent a century ago, when Picasso was pasting oil cloth and newspaper clippings onto canvases. It certainly existed long before that, when Aristophanes was parodying the writings of Euripides and Sophocles, to when Dante was reimagining Virgil, and later when Shakespeare was seemingly freely borrowing from the entirety of English literature [Suzor, 2005].

In the UGC environment end-users (consumers) present an uncommonly active role in the production process. Put it differently, consumers produce. This new kind of users (commonly referred to as Prosumers,) constitutes an integral part of the digital citizens and plays a crucial role to the development of Information Society [Elkin-Koren, 2009]. Prosumers seem to present certain characteristics associated with the reasons for which UGC is produced. Thus, they are firstly animated by amateurism. Even if they are professionals, one could no longer deny the fact that a remixed song composed by a professional musician on the basis of a pre-existing one and then displayed publicly on the Web for free serves no more any professional goal. Moreover, it seems that Prosumers have a need in sharing their derivative works. Most of the social networking sites or distribution platforms (or even peer to peer networks to the extent that "derivative works" are uploaded) are commonly understood as "recreation rooms" of the digital world, where end - users wish to criticize opinions, comment on posted materials or just entertain themselves along with the users of the rest community. Finally, Prosumers seem to be susceptible to collaborative efforts rather than individual ones. Wikipedia offers an excellent paradigm of this trend: users create a collective work due to their personal contributions (much of which may be regarded as derivative works and consequently UGC).

## Facing Copyright

In the UGC environment, the user is able to do "almost everything". He is able to upload and download "user – created" works based on existing copyrighted ones to peer to peer networks, distribution platforms or social networking sites. He

is also able to post "articles" and other content on bulletin boards or other web-hosting sites. But most importantly, the key-element in the Age of UGC is that all of these acts can take place in most cases "for free", that is, without payment to the alleged proprietor of the "content" (or part thereof).[1] In this context, one should bear in mind that the "posted" content may be protected (either in full or in part) by intellectual property rights and most importantly, by copyright and/or its related rights.

In view of the broadened extent of the phenomenon at question with regard to copyright law, the analysis of this Part will be classified into two categories, that is, evaluating from a legal point of view: the act of interfering with an existing copyrighted work and creating a derivative one (under 2.1.) and the act of uploading such a derivative work (under 2.2.). The analysis will also focus to the economic exclusive rights of the relevant right holders with particular emphasis to the EU legal framework.

### *Interfering with an existing copyrighted work – production of a "derivative" work*

Many acts in the UGC environment may constitute the subject-matter of exclusive rights in existing copyrighted works. *Remixing* or *sampling* and *mash-ups* (taking a digital media file containing any or all of text, graphics, audio, video and animation drawn from pre-existing sources to create a new derivative work) would be definitely acts covered by the copyright owners' exclusive rights.

#### The Reproduction Right in the International framework

Article 9 (1) of the Berne Convention titled Right of Reproduction states:

> "Authors of literary and artistic works protected by this Convention shall have the exclusive right of authorizing the reproduction of these works, in any manner or form"

At the same time Article 9 (3) of the Berne Convention is explicitly referred to sound or visual recordings to be considered as "reproductions" for the purpose of the Berne Convention.

Furthermore, the Guide to the Berne Convention explains that: "The words "…in any manner or form" are wide enough to cover all forms of reproduction: design, engraving … and all other processes known or yet to be discovered" [Guide to the Berne Convention, 1971].

On the other hand, the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) of 1994, specifically incorporated Article 9 (1) of the Berne Convention into its Article 9. The main legal conse-

quence is that countries that defectively implement the "reproduction right" provision of the Berne Convention risk running afoul of their TRIPS obligations and becoming subject to dispute settlement.

The WIPO Copyright Treaty of 1996 (WCT) and the WIPO Performances and Phonograms Treaty of 1996 (WPPT) (collectively referred to as Internet Treaties) also contain provisions as regards the reproduction right. 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. In the Agreed statements concerning Article 1(4) of the WCT it is stated:

> "The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder, fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention."

The provision of Article 7 in conjunction to that of Article 11 of the WPPT reads:

> "Performers [Producers of phonograms] shall enjoy the exclusive right of authorizing the direct or indirect reproduction of their performances fixed in phonograms [phonograms], in any manner or form."

Similarly, the Agreed statement concerning Articles 7, 11 and 16 of the WPPT states:

> "The reproduction right, as set out in Articles 7 and 11, and the exceptions permitted thereunder through Article 16, fully apply in the digital environment, in particular to the use of performances and phonograms in digital form. It is understood that the storage of a protected performance or phonogram in digital form in an electronic medium constitutes a reproduction within the meaning of these Articles."

In the light of the provisions above, one may clearly suggest that all of the acts of artistic appropriation into which end- users engage may infringe the initial creators' exclusive right of reproduction. More specifically, the acts of remixing or sampling and mashing up consist in two technical steps, that is, the copyrighted material (or portions thereof) should be obtained and then should be subjected to interference by the end-user.

To obtain a copyrighted work in the electronic environment means that the work (data) should be received and stored in a device that is controlled by the end-user, either a permanent or a temporary one.[2] A usual way of receiving data from the Web is to download it. The act of downloading is usually accompanied by the subsequent act of storage of the data in a permanent storage device (e.g. the

personal computer's hard disk or a CD, DVD, memory stick etc). After the work in question is stored, it is then capable of being modified by the end- user. For example, the act of remixing presupposes: the act of downloading a song in question (or part thereof) [receiving], the subsequent act of storing it on a permanent storage device (e.g. hard disk) [storage] and the act of interfering with it in order to "build" a new "derivative" music [interference]. The first two acts purport at obtaining the copy of a song and the third act aims at interfering with it.

In the light of the provisions above, to obtain a copyrighted work without the owner's prior authorization constitutes – in the digital environment - a direct infringement of the exclusive right of reproduction, since the necessary action of storing the data in a permanent storage device is expressly covered by the reproduction right. It is also important to note that even certain acts of interference may constitute the subject-matter of the reproduction right on top of storing the copyrighted work. For example, in the case of remixing the – after downloading and storing - subsequent act of recording the copyrighted sound (or part thereof) clearly infringes the owner's exclusive reproduction right (either in full or in part) by virtue of Article 9 (3) of the Berne Convention.

## The reproduction right in the European framework

Copyright law is not yet harmonized across the EU Member States. However, the existing regulatory framework in the context of the information society consists basically of Directive 2001/29.[3] According to the provisions of this Directive, a copyright owner retains - in the context of information society - the following exclusive rights: 1) the reproduction right[4] 2) the right of communication to the public of works and the right of making available to the public other subject-matter[5] and 3) the distribution right.[6]

As to the reproduction right, Article 2 of the Directive reads:

"Member States shall provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part:

(a) for authors, of their works;

(b) for performers, of fixations of their performances;

(c) for phonogram producers, of their phonograms;

(d) for the producers of the first fixations of films, in respect of the original and copies of their films;

(e) for broadcasting organisations, of fixations of their broadcasts, whether those broadcasts are transmitted by wire or over the air, including by cable or satellite."

It is important to note that the formulation of Article 2 is quite broadened. The reproduction right is wider in its definition than it internationally is for authors (Berne Convention) and holders of related rights (WPPT, TRIPS) [IViR, 2007]. This is explained by the legislation itself, which states in recital 21 in its preamble that 'a broad definition of these acts is needed to ensure legal certainty within the internal market'.

Nevertheless, Article 2 seems to encompass the notion of "partial reproduction" within the sphere of the reproduction right. Indeed, this is probably the most important implication of the Directive towards acts that "reproduce in part" a copyrighted work. In *Infopaq International A/S v Danske Dagblades Forening*[7] the ECJ (after receiving a reference for a preliminary ruling from the Danish Court) recently ruled that an act occurring during a data capture process, which consists of storing an extract of a protected work (daily newspaper article) comprising 11 words and printing out that extract, is such as to come within the concept of reproduction in part within the meaning of Article 2 of Directive 2001/29, if the elements thus reproduced are the expression of the intellectual creation of their author [Recital 51]. The Court however noted that it is for the national court to make this determination. [Recital 51].

The reasoning of the Court is indeed useful in applying the rules of copyright to acts that relate to UGC. It seems that remixing, sampling or mashing up are surely acts covered by the reproduction right (in part) within the meaning of Article 2 of the Directive, if the part of the work is such as to express the author's own intellectual creation. In other words, if the referring national court finds out that the extract of 11 words constitutes "…an element of the work which, as such, expresses the author's own intellectual creation…" or that such extract "…may be suitable for conveying to the reader the originality of a publication such as a newspaper article, by communicating to that reader an element which is, in itself, the expression of the intellectual creation of the author of that article…", then there will be no doubt that, by analogy, the storing of a part of a musical work, which, by itself, expresses the owner's intellectual creation, will definitely constitute an act that "reproduces partially" the original copyrighted work within the meaning of Article 2 of the Directive.[8]

## Translation and adaptation rights

Closely related to the right of reproduction is the right of adaptation, which provides copyright holders with the right to adapt a copyrighted work from one form of expression to another, or to authorize another to do so.

According to Article 12 of the Berne Convention "…Authors of literary or artistic works shall enjoy the exclusive right of authorizing adaptations, arrangements

and other alterations of their works." Examples of adaptations include transforming a book into a movie or a song into a musical. The right of adaptation is also found in virtually all copyright systems. For example, Article 12 of the Berne Convention requires member countries to grant authors the right to authorize "adaptations, arrangements, and other alterations of" copyrighted works. The right of adaptation also encompasses the right to translate a work into other languages. Article 8 of the Berne Convention requires member countries to recognize this right of translation. In some legal systems, the right of adaptation is expressed as the right to make "derivative works," which use the original work as a starting point but are not direct copies of the original work.

In most countries, the reproduction right and the adaptation right are closely aligned. In other words, the majority of activities that violate the adaptation right also violate the reproduction right. However, there are exceptions. For example, cutting up a photograph to include it in a collage may violate the adaptation right (unless of course that behavior is excused by one of the exceptions or limitations). But, because that activity did not entail making a new copy, it would not violate the right of reproduction. However, the degree of overlap between these two rights varies somewhat by country. Which of the two rights is implicated by a particular case will sometimes make a difference; for example, if the copyright owner has granted a license for one of the rights but not the other [Harvard, 2009].

Most acts in the UGC world are probably covered by the "adaptation right". However, it is important to note that copyright only protects the expression of ideas, not the ideas or facts themselves. Thus, it is self-explanatory that a work that is inspired by the ideas contained in another work but does not use any of the protected expression from the initial work is neither a reproduction nor an adaptation, and will not violate the copyright holder's rights. In that regard, Article 2(3) of the Berne Convention provides that authorized adaptations are protected by their own separate copyright, in addition to the copyright protection given to the original work [Markellou, 2009].

The scope of the right of adaptation has been the subject of significant discussion in recent years because of the greatly increased possibilities for adapting and transforming works which are embodied in digital format. These discussions have focused on the appropriate balance between the rights of the author to control the integrity of the work by authorizing modifications, and the rights of users to make changes which seem to be part of a normal use of works in digital format [WIPO, 2009].

### *Uploading a "user-generated" work*

The act of uploading a transformed copyrighted work to the Web could possibly be an act that constitutes the subject-matter of right holder's two exclusive economic rights: a) the right of communication to the public of a protected work and b) the right of making available to the public a protected work

## The right of "communication to the public" and the right of "making available to the public" in the international framework

The exclusive right of communication to the public was provided for by Articles 11 (1) (ii), 11bis (1) (i) and (ii), 11ter (1) (ii), 14 (1) (ii) and 14bis (1) of the Berne Convention, which conferred such right to authors of literary and artistic works but confined to performances, broadcasts, and recitations of works.

The new WIPO Internet Treaties (WCT and WPPT) provide for a broader definition of the communication right. In particular, Article 8 of the WCT provides:

> "Without prejudice to the provisions of Articles 11(1)(ii), 11bis(1)(i) and (ii), 11ter(1)(ii), 14(1)(ii) and 14bis(1) of the Berne Convention, authors of literary and artistic works shall enjoy the exclusive right of authorizing 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 these works from a place and at a time individually chosen by them."

In a first place, it seems that the wording of the abovementioned provision suggests that the "making available to the public" right is included in the broader context of the exclusive right of communication to the public.

At the same time, Articles 10 and 14 of the WPPT applies the communication right to performers and producers of phonograms. The WPPT defines these rights as ones of "making available to the public". Article 10 [and 14] of the WPPT provides:

> "Performers [producers of phonograms] shall enjoy the exclusive right of authorising the making available to the public of their performances [phonograms], by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them."

After the adoption of the abovementioned provision it seemed that there was little doubt to claim that the "making available to the public" right is not an exclusive one at least as regards the performances and phonograms. In fact, the WIPO Internet Treaties broadened the extent of "the communication to the public" right, by introducing a new exclusive right of "making available to the public" copyrighted works. However, the Treaties left open the possibility to implement

those provisions into the national legislations either on the basis of an existing exclusive right or through enactment of a new right [IFPI, 2003].

The broad formulation of the Internet Treaties' provisions as to the "making available right" covers all types of exploitation that allow consumers to have a choice as to the time and place to enjoy copyrighted content on-line. Thus, the implementing legislation should cover all services that allow e.g. the listening of music, the download of permanent copies of music tracks, on-demand services or other services with a like effect.

Moreover, the act of "making available" could be achieved by all means of delivery, either by wire or wireless means, but in such a way that members of the public may access the work or phonogram from a place and at a time individually chosen by them.

The "making available" right covers both the actual offering of the phonogram or other protected material and its subsequent transmission to members of the public. In other words, the act of "making available" is subject to the control of the phonogram producer or other rights owner from the moment the work or phonogram is accessible to members of the public, regardless whether it has been accessed or not. Put it differently, it is the accessibility of the content (that being capable for being received by the public) the decisive factor for an act to be caught by the provisions of the WIPO Internet Treaties.

In the light of foregoing, the act of uploading (for example) a part of a copyrighted song to a distribution platform (e.g. YouTube) is probably covered by the exclusive right of "making available to the public", since even the mere fact of uploading seems to be sufficient for the copyrighted content to be accessible by a considerable portion of the public, which has a choice as to the time and place to enjoy such content on-line.

On the contrary, as the Agreed statements concerning Article 8 of the WCT provides "the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention." This essentially means that internet service providers that provide a mere access to a network could not be regarded as infringers of the exclusive "making available right" of the respective copyright owner [WIPO, 2005].

## The right of "communication to the public" and the right of "making available to the public" in the European Framework

Article 3 (1) of the InfoSoc Directive provides authors with the exclusive right to authorise 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. This paragraph reflects the international obligation of the European Communities as envisaged by Article 8 of the WCT.[9]

At the same time paragraph 2 of the same Article confers to performers, phonogram producers, producers of the first fixations of films and broadcasting organisations the exclusive "making available right", by wire or wireless means, as that envisaged in the first paragraph of that article. This second paragraph reflects the Communities' obligations in the light of Article 10 [and 14] of the WPPT. [10]

The European Commission opted in introducing this new "making available right" as a new exclusive one. It is further important to note that the "making available" right, as envisaged in Article 3 of the Directive conforms to WCT and WPPT norms, albeit that those instruments do not recognize a "making available right" for producers of the first fixations of films and broadcasting organisations [IViR, 2007].

The purpose of the making available right is, in legal terms, to ensure that copyright law applies to digital services on demand, that is, works selected interactively by the consumer at a time and place of her choosing [Recitals 23 to 27, Towse 2003].

The scope of application of Article 3 of the Directive 2001/29/EC in terms of the right to communication to the public was considered by the European Court of Justice (the "ECJ") in *Sociedad General de Autores v Editores de España (SGAE) v Rafael Hoteles SA*.[11] SGAE, the body responsible for the management of intellectual property rights in Spain, complained that the installation and use of television sets in the Rafael hotel involved the communication to the public of works falling within the repertoire which it managed. The national Spanish Court referred to the ECJ for a preliminary ruling on whether: a) the transmission of a broadcast signal through television sets to customers in hotel rooms constitutes communication to the public within the meaning of Article 3(1) and b) the mere installation of television sets in hotel rooms constituted such an act.

The ECJ thought that a communication made in circumstances such as those constitutes, according to Art.11bis (1) (ii) of the Berne Convention, a communication made by a broadcasting organisation other than the original one. Thus, such a transmission is made to a public different from the public at which the original act of communication of the work is directed, that is, to a new public [Recital 40]. The clientele of a hotel forms such a new public [Recital 41]. In line to what has mentioned above about acts to be regarded as "making available", the ECJ noted that:

> "...It follows from Art.3(1) of Directive 2001/29 and Art.8 of the WIPO Copyright Treaty that for there to be communication to the public it is sufficient

> that the work is made available to the public in such a way that the persons forming that public may access it. Therefore, it is not decisive, contrary to the submissions of Rafael and Ireland, that customers who have not switched on the television have not actually had access to the works."[12]

Moreover, reflecting the underlying concept of the Agreed statements concerning Article 8 of the WCT and recital 27 of the Directive (in ruling on the second question referred) the ECJ stressed:

> "…While the mere provision of physical facilities, usually involving, besides the hotel, companies specialising in the sale or hire of television sets, does not constitute, as such, a communication within the meaning of Directive 2001/29, the installation of such facilities may nevertheless make public access to broadcast works technically possible. Therefore, if, by means of television sets thus installed, the hotel distributes the signal to customers staying in its rooms, then communication to the public takes place, irrespective of the technique used to transmit the signal."[13]

Despite the guidance offered by the ECJ in its ruling in *Sociedad General de Autores v Editores de España (SGAE) v Rafael Hoteles SA*, there is no case law at a community level to answer to the obvious question on whether the right of communication to the public and that of making available to the public (both as to authors and as to performers, phonogram producers, producers of the first fixations of films and broadcasting organisations) should cover the communication (or the making available) to the public of *a certain part of the protected work* in question.

Indeed, in the UGC context one should answer the question of whether the act of uploading a transformed copyrighted work infringes the owner's exclusive rights of communication to the public and/or that of making available to the public the protected work *only as regards the part of it that is "used" by the end-user*. For example, when uploading a remixed song, the user actually uploads the combination *of a (substantial) part of a pre-existing song* along with a personal music composition.

As already pointed out above (under 2.1.) the reproduction right covers the act of storing either the work in whole or a certain part thereof. In view of the ruling of the Court in Infopaq International A/S v Danske Dagblades Forening and the language of the Directive itself in Article 2 ("…in whole or in part…"), a "partial reproduction" is possible within the EU legal framework. This is, however, not the case in terms of the right of communication to the public and that of making available to the public, since such wording is missing in Article 3 of the InfoSoc Directive. Unless an interpretative legal instrument suggests that a "partial communication" is an acceptable legal concept in the EU legal order, it would be

rather difficult to assume that user – created content infringes the owner's exclusive broad "communication to the public" rights.

## Limitations on Copyright

As already seen in the previous part, the act of obtaining a permanent copy[14] of a work in question (or a part thereof) constitutes a direct infringement of the owner's exclusive right of reproduction (either in full or in part). It is also understood that certain acts of interference violate the right of adaptation and in some cases the exclusive right of reproduction, as well. [15] Finally, in the light of artistic appropriation, into which end-users engage, it is not clear whether the newly created derivative work infringes the right of communication to the public and/ or the right of "making available to the public", since the language of Article 3 of the InfoSoc Directive does not provide any argument in favour of the "partial communication" concept, as it expressly does in Article 2 with regard to the reproduction right.

But copyright law, as any other kind of law is not absolute. Under certain circumstances and to the extent that certain conditions are met, it allows limitations or exceptions to its rules.

### *Existing exceptions and limitations on Copyright of relevance to UGC*

Article 5 (1) of the InfoSoc Directive provides for a mandatory[16] exception as to the reproduction right in terms of temporary acts of reproduction that are purely transient or incidental [and] an integral and essential part of a technological process, that are of no independent economic significance. As Recital 33 of the Directive explains "…this exception should include acts which enable browsing as well as acts of caching to take place, including those which enable transmission systems to function efficiently". However, in view of the fact that copyrighted works have to be stored in a permanent storage device in order to be subject to interference by the end-user, this exception is far from applicable in the case of UGC acts.

Furthermore, Article 5 (2) and (3) of the Directive does provide an exhaustive list[17] of optional[18] exceptions in the exercise of each one of the abovementioned exclusive rights. Of those, one may identify two possible exceptions associated with acts in the UGC context, namely: i) those acts that constitute "…quotations for purposes such as criticism or review" provided for by Article 5 (3) (d) and ii) uses that intend to "…caricature, parody or pastiche…" provided for by that article 5 (3) (k).

The first exception appears rather imprecise. On the author's opinion, the concept of the UGC, as phenomenon, appears much greater than the concept of the

relevant exception. In other words, Article 5 (3) (d) refers to a typical case of quoting a copyrighted work for various purposes, while in our case the end-user engages into a creative effort to create a derivative work.

On the other side, the implementation of the parody exception in national laws varies. For example, there is no parody exception under UK law. In contrast, other national laws expressly provide for a parody exception (for example France, Belgium) or cover parodies under the umbrella of transformative use (Nordic countries) or of a free use defence (Germany[19] and Portugal for example) [Commission document, 2007].

Thus, the Commission correctly argues that none of the exceptions provided for by the Directive may relate to content originated by the user [Commission document, 2007].

The European Commission has long before identified that a legitimate exploitation of users-generated content, as part of the so called "creative content distributed online" will definitely present many advantages within the borders of the EU both from an economic and a social perspective [Communication from the Commission, 2007]. However, the creation of new or derivative works or the interference with existing copyrighted works remains a central issue to be resolved at a community level [Commission Document, 2007]. Thus, the European Commission has issued a Green Paper on Copyright in the Knowledge Economy calling for proposals on two basic issues: 1) whether there should be more precise rules on what exactly is permitted to the end-user to do when interfering with copyrighted material on line and 2) whether an exemption regarding user –created content should be introduced in Directive 2001/29 [Green Paper, 2008]. Towards such an effort the Commission received many responses. All of them indicated, however, that it is too early to regulate UGC, because it is both unclear on whether amateurs and professionals should benefit from special rules on UGC and how rules on UGC would relate to existing limitations, such as quotations, incidental use, and "caricature, parody or pastiche" [Communication from the Commission, 2009].

At the same time, the European Council has invited the member states to launch consultations on finding solutions to develop legal offers of creative content on line and protecting the original creators' rights on existing copyrighted works [Council Conclusions, 2008]. In this context, however, the most important development seems to be the recent discussion within the EU on adopting a legal instrument on European Copyright, thereby regulating the matter in a uniform way, according to the principles of EU law including the principle of proportionality [Opinion, 2007].

### *The "three-step test" as the "limitation of limitations"*

Anyway, it should be important to note at this point that even if an exception is to be introduced, either in a European or a national level, such an exception has to be in conformity with Article 5 (5) of the Directive, which states:

> "The exceptions and limitations provided for in paragraphs 1, 2, 3 and 4 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."

Recital 44 of the Directive offers guidance in terms of Article 5 (5) of the Directive:

> "…When applying the exceptions and limitations provided for in this Directive, they should be exercised in accordance with international obligations. Such exceptions and limitations may not be applied in a way which prejudices the legitimate interests of the right holder or which conflicts with the normal exploitation of his work or other subject-matter. The provision of such exceptions or limitations by Member States should, in particular, duly reflect the increased economic impact that such exceptions or limitations may have in the context of the new electronic environment. Therefore, the scope of certain exceptions or limitations may have to be even more limited when it comes to certain new uses of copyright works and other subject-matter."

It is obvious that Recital 44 and Article 5 (5) of the Infosoc Directive reflect an international obligation of the European Communities, well known as the "Three-Steps test".

The "three-steps test" first appears in Article 9 (2) of the Berne convention (in terms of the reproduction right), which states:

> "It shall be a matter for legislation in the countries of the Union to permit the reproduction of such works in certain special cases, provided that such reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author."

This provision is considered to be the "limitations' limitation", in the sense that contracting parties may introduce exceptions in their national legislations, insofar as those exceptions pass successfully the relevant test.

The TRIPS Agreement also extended the scope of the "three step test" of the Berne Convention in its Article 13 [by virtue of its Article 9 (1)] concerning any rights in literary and artistic works. Article 13 titled (Limitations and Exceptions) of the TRIPS reads:

> "Members shall confine limitations or exceptions to exclusive rights to certain special cases which do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the right holder.

In addition, Article 10(2) of the WCT, similarly to Article 13 of the TRIPS Agreement, extends the application of the three-step test to all economic rights provided in the Berne Convention, while Article 16(1) of the WPPT provides that Contracting Parties may introduce "the same kinds of limitations and exceptions with regard to the protection of performers and producers of phonograms as they provide for, in their national legislation, in connection with the protection of copyright in literary and artistic works".

An agreed statement was adopted concerning Article 10 of the WCT on limitations and exceptions, which reads as follows:

> "It is understood that the provisions of Article 10 permit Contracting Parties to carry forward and appropriately extend into the digital environment limitations and exceptions in their national laws which have been considered acceptable under the Berne Convention. Similarly, these provisions should be understood to permit Contracting Parties to devise new exceptions and limitations that are appropriate in the digital networked environment. It is also understood that Article 10 (2) neither reduces nor extends the scope of applicability of the limitations and exceptions permitted by the Berne Convention."

This agreed statement is applicable, mutatis mutandis, also concerning Article 16 of the WPPT on limitations and exceptions.

This agreed statement requires appropriate interpretation. Both Article 10 of the WCT and Article 16 of the WPPT prescribe the application of the same three-step test as a condition for the introduction of any limitation on or exception to the rights granted by the Treaty as what is provided in Article 9 (2) of the Berne Convention concerning the right of reproduction and in Article 13 of the TRIPS Agreement concerning any rights in literary and artistic works. Thus, any limitation or exception may only be introduced (i) in a certain special case; (ii) if it does not conflict with a normal exploitation of the works, performances or phonograms, respectively; and (iii) if it does not unreasonably prejudice the legitimate interests of the owners of rights.

The WIPO study on the "Implications of the TRIPS Agreement on Treaties Administered by WIPO" refers to the fact that "[t]he Berne Convention contains a similar provision concerning the exclusive right of reproduction (Article 9(2)) and a number of exceptions or limitations to the same and other exclusive rights (see Articles 10, 10bis and 14bis(2)(b)) and, it permits the replacement of the exclusive right of broadcasting, and the exclusive right of recording of musical works, by

non-voluntary licenses (see Articles 11bis(2) and 13(1))." After this, it states the following: "None of the limitations and exceptions permitted by the Berne Convention should, if correctly applied, conflict with the normal exploitation of the work and none of them should, if correctly applied, prejudice unreasonably the legitimate interests of the right holder. Thus, generally and normally, there is no conflict between the Berne Convention and the TRIPS Agreement as far as exceptions and limitations to the exclusive rights are concerned." [WIPO, 1997]

As indicated in that analysis, the application of the three-step test for the specific limitations and exceptions allowed by the Berne Convention is an interpretation tool: it guarantees the appropriate interpretation and application of those limitations and exceptions.

On the basis of this analysis, it is clear that what the above-quoted agreed statement refers to – namely the carrying forward and appropriate extension into the digital environment of limitations and exceptions "which have been considered acceptable under the Berne Convention"– should not be considered an automatic and mechanical exercise; all this is subject to the application of the three-step test. The conditions of normal exploitation of works are different in the digital environment from the conditions in a traditional, analog environment, and the cases where unreasonable prejudice may be caused to the legitimate interests of owners of rights may also differ. Thus, the applicability and the extent of the "existing" limitations and exceptions should be reviewed when they are "carried forward" to the digital environment, and they may only be maintained if -- and only to the extent that -- they still may pass the three-step test [WIPO, 2003].

The concept of the "three-step test" was considered for once by the WTO Panel in United States – Section 110(5) of the US Copyright Act.[20] In that case, the European Communities requested consultations with the United States of TRIPS Agreement, regarding Section 110(5) of the United States Copyright Act, as amended by the "Fairness in Music Licensing Act" enacted on 27 October 1998. In particular, the US provisions actually provided for a limitation on the owners' exclusive rights towards two directions: a) to communicate a transmission embodying a performance or display of a work by the public reception of such transmission on a single receiving apparatus of a kind commonly used in private homes[21] and b) to communicate by an establishment of a transmission or retransmission embodying a performance or display of a non-dramatic musical work intended to be received by the general public just in case that certain conditions were to be met.[22] Those provisions were claimed by the European Communities to be incompatible to Article 11bis(1) of the Berne Convention and the discussion of the case was inevitably led to the issue of whether the provisions of the

US copyright law successfully pass the three-step-test as that envisaged at last in Article 13 of the TRIPS Agreement.

The Panel noted that, firstly, these three conditions apply cumulatively; a limitation or an exception is consistent with Article 13 only if it fulfils each of the three conditions.[23]

In the Panel's view, the first step of Article 13 ("…certain special cases…") requires that a limitation or exception in national legislation should be clearly defined and should be narrow in its scope and reach. On the other hand, a limitation or exception may be compatible with the first condition even if it pursues a special purpose whose underlying legitimacy in a normative sense cannot be discerned. The Panel also notes that the wording of Article 13's first condition does not imply passing a judgment on the legitimacy of the exceptions in dispute. However, it stated that public policy purposes stated by law-makers when enacting a limitation or exception may be useful from a factual perspective for making inferences about the scope of a limitation or exception or the clarity of its definition.[24]

As regards the second step of Article 13 ("…do not conflict with a normal exploitation of the work…") the overall assessment of the Panel was reflected in that an exception to a right rises to the level of a conflict with a normal exploitation of the work, if uses, that in principle are covered by the right, but exempted by the exception, enter into economic competition with the ways in which right holders normally extract economic value from that right, and thereby deprive them of significant or tangible commercial gains.[25] At this point, it is also of crucial importance to note that the Panel thought that the condition of the "normal exploitation" of a work has to be judged for each right granted under copyright individually, rather than in the context of the entire rights conferred by copyright in a work.[26] Finally, the WTO Panel felt that it is the potential damage caused by an exception which is relevant to deciding whether it conflicts with normal exploitation, rather than the actual damage occurring at a particular time [WIPO, 2000].

With regard to the third step of Article 13 ("…do not unreasonably prejudice the legitimate interests of the right holder …") the overall conclusion of the Panel was that prejudice to the legitimate interests of the right holders reaches an unreasonable level if an exception causes, or has the potential to cause, an unreasonable loss of income to the right holder. [27] In practical terms, what the Panel was driving at, is that it is the scale of losses to the right owners which is the determining factor in judging whether an exception is unreasonable, and again it emphasized that is potential, rather than actual losses, which in its view are relevant [WIPO, 2000].

### *The "three - step test" and the "user-created content" exception*

Having in mind the interpretation of the three step test, as envisaged in the WTO Panel's Report in United States – Section 110(5) of the US Copyright Act, there is probably little to say about the compatibility of acts related to UGC to the three steps of Article 13 of the TRIPS Agreement. Indeed, even if European legislators introduce an exception to the harmonised exclusive rights of the right holders in terms of content originated by the user, I personally do not think that there is still any possibility to pass the three step test successfully.

First of all, exceptions or limitations to the reproduction and/or adaptation rights in the course of acts of remixing/sampling or mashing up should be clearly defined and should be narrow in its scope and reach. That, however, could be possible if the relevant legislation pursues a special purpose (e.g. the creativity as a basic parameter for the dissemination of culture). As follows from the careful reading of the report, public policy reports could assist towards the direction of clarifying the purpose for which the exception of user-generated content is pursued.

Nevertheless, the matter seems to be much more complicated with regard to the second step. To consider an exception as a "normal exploitation", the exempted use, that in principle is covered by the right, but exempted by the exception, should not enter into economic competition with the ways in which right holders normally extract economic value from that right and thereby does not deprive them of significant or tangible commercial gains (a contrario). Whereas this test is applied to each of the exclusive rights separately, is it safe to assume that the downloading of a copyrighted song, or the subsequent recording of a copyrighted sound (acts covered by the reproduction right) does not deprive copyright owners of significant or tangible commercial gains? Or could someone claim convincingly that the subsequent alteration or modification of the copyrighted subject-matter with a view to creating a new derivative work (acts covered by the adaptation right) does not enter into economic competition with the ways in which the copyright owner normally extracts economic value from the (adaptation) right? The answer is, in my view, absolutely negative. Things are also getting worse, if we recall that it is the potential damage caused by an exception which is relevant to deciding whether it conflicts with normal exploitation, rather than the actual damage occurring at a particular time.

The same applies, mutatis mutandis, as to the third step of the relevant test ("... do not unreasonably prejudice the legitimate interests of the right holder ...").

There is plenty of academic literature criticizing the much restrictive interpretation of the "three - step test" adopted by the Panel in United States – Section 110(5) of the US Copyright Act. As many commentators point out, a restrictive

approach of the "three - step test", risks paralysing the development of copyright exceptions and harming the public interest in the digital environment [Geiger, 2007]. If the three conditions of the test are interpreted as cumulative requirements and if the second step is interpreted restrictively as precluding most interventions into a right holder's market, there is a danger that the prohibition upon all conflict with a normal exploitation of a work will assume undesirable "show-stopping" status [Koelman, 2006]. In other words, whenever an excepted use deprives the right holder of a realisable commercial gain (current or potential), the second step will be infringed and the application of the exception will necessarily be curtailed, regardless of any competing public interest consideration that the exception at issue may serve [Griffiths, 2009]. Thus, as Ginsburg argues: "…even traditionally privileged uses, such as scholarship or parody, could be deemed "normal exploitations", assuming copyright owners could develop a low transaction cost method of charging for them" [Ginsburg, 2001].

As far as the digital technology is concerned, it should also be noted that, as a broader range of means of exploitation of copyright works becomes technically feasible, the scope of the potential "normal exploitation of a copyright work correspondingly increases and if a restrictive approach to the second step is adopted, the discretion of states (and courts) to maintain appropriately fashioned exceptions is diminished [Senftleben, 2004].

At a European level, it should be emphasized that it is also not clear whether Article 5 (5) of the InfoSoc Directive - encompassing the three step test - forms a rule directing to national legislatures or to the national courts. The distinction is of crucial importance, since the former would enable legislators themselves to enact "certain special" exceptions that would a priori fit to the three step test. On the contrary, if Article 5 (5) is a rule of "judicial review" that would undoubtedly form a powerful interpretative tool to define the legitimacy of the copyright exception in question [Griffiths, 2009]. However, the signs of the lack of a uniform application of the three step test have already arrived. There is much case law across the member states - some of which have implemented Article 5 (5) of the Directive literally in their national legislation - that indicates the divergent approaches taken by the court across the European Continent [Griffiths, 2009].

There are many proposed solutions as to the problems that arose due to the restrictive interpretation of the three step test that the WTO Panel adopted in its Report in United States – Section 110(5) of the US Copyright Act. Many of them seem to suggest the re-writing of the International Treaties, but this seems to be too optimistic a scenario, since the legislative process is a time-consuming and hard process at least in an international level. Others, however, seem to opt in offering new interpretative analysis of the test.

Of particular interest seems to be a recent declaration issued jointly by the Max – Planc Institute and the University of Queen Mary, London [Phillips, 2008]. The main concepts of the Declaration may be summarized in the following elements, namely that: i) the three steps are nothing, but individual elements informing one overall assessment ii) the limitations and exceptions are to be interpreted according to their objectives and purposes iii) legislatures and courts may introduce open ended exceptions under certain conditions iv) the limitations and exceptions do not conflict with a normal exploitation of a protected subject-matter if they are based on important competing considerations or have the effect of countering unreasonable restraints on competition v) in applying the three step test account should be taken into the interests of the right holders and the interests of subsequent right holders (users) vi) the test should be applied in a manner that respects the legitimate interests of third parties [Declaration, 2008].

The Declaration seeks to offer a balanced interpretation of the Three-Step test and is, at the time of writing, signed by leading scholars in the field of Intellectual Property. Unless the European Legislature or the European Courts of Justice adopt the much needed flexible approach of the test, exercising in that regard its explanatory power, the three step test will operate in the future copyright laws against the public interest and as an unjustifiable curtailment over justified exceptions and limitations.

## Concluding Remarks: Two worlds collide?

The analysis into which the author of this contribution engaged focused on the newly apparent phenomenon of user – created content and its relationship with the existing copyright laws.

In the first part of it, we mentioned that due to Web 2.0 technologies users are able to upload content that is neither of their personal exclusive creation nor of other existing ownership. Instead, consumers base their creations on existing copyrighted works in order to create new derivative ones, by combining the former with a personal contribution. This newly introduced content originated by the user (the Prosumer) is commonly referred to as "user created/generated content" and plays quite an important role in the dissemination of the so – called "mashing up" culture within the information society. Alongside, Prosumers present an uncommonly active role in such a process thereby contributing to the development of "the production process" within the Information Society.

However, and to the extent already discussed in the second part of our analysis, the course of acts into which end-users engage in order to create new derivative works, infringe the owner's exclusive economic rights. Of those, the reproduction right and the right of adaptation seem to be the most vulnerable towards the acts

of remixing and mashing-up, while it is not clear whether the newly created derivative work infringes the right of communication to the public and/or the right of "making available to the public". Those rights are provided for by International Treaties and the rules governing them are harmonized across the EU Member states by virtue of the provisions of the InfoSoc Directive.

On the contrary, as the third part mentioned, certain rules within the EU legal framework allow for possible exceptions under copyright laws, but still none of them may be relevant to UGC. Thus, the European Commission launched a consultation on whether acts related to content originated by the user may be specifically exempted from the application of the owner's exclusive rights.

Despite the fact that the recent responses stated the opposite, the author discussed such a possibility and went on to analyze the compatibility of such a possible exception in the light of the "three step test", as that envisaged by Article 13 of the TRIPS Agreement. The Three-Step test defines the scope of the application of the exceptions and limitations, so that an exception to the copyright laws must successfully pass it in order to be considered as lawful. Unfortunately, the much restrictive interpretation of the "three - step test" adopted by the Panel in United States – Section 110(5) of the US Copyright Act, leaves no possibility for the relevant exception to be compatible to Article 13 of the TRIPS Agreement. It seems that at this point of analysis that the "user created content" exception loses the battle against the copyright law.

But that last statement may be of some relevance. The much restrictive interpretation of the "three - step test" adopted by the Panel in United States – Section 110(5) of the US Copyright Act and the lack of a teleological interpretation gave rise to a considerable part of society (users and especially academics) to form a balanced interpretation of the Three-Step test that takes into serious account the concept of the "public interest". If such an approach is finally adopted by the official EU legislature, or better by the European Courts of Justice - exercising in that regard its explanatory power - there will be no question that the "user created content" exception lost a battle but not the war against the exclusivity power of copyright law.

## References

IFPI (2003), The WIPO Treaties: the "making available right", online at http://www.ifpi.org/content/library/wipo-treaties-making-available-right.pdf/ accessed 20.05.2010

Carlisle George, Jackie Scerri, (2007), "User-generated content on - line: Legitimate power or the wild west?", Annual Conference 2007, BILETA, Hertfordshire,

UK, online at: http://www.bileta.ac.uk/Document%20Library/1/User-Generated%20Content%20Online%20%20Legitimate%20power%20or%20the%20Wild%20West.pdf accessed 20.05.2010

Commission staff working document, (2007) "Report to the Council, the European Parliament the Economic and Social Committee on the application of Directive 2001/29 on the harmonization of certain aspects of copyright and related rights in the information society", SEC/2007/1556

Commission staff working document, (2007), Document accompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on creative content online in the Single Market, COM(2007) 836 final SEC/2007/1710 final

Commission staff working document, Document accompanying the Communication from the Commission, the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, SEC (2009), 1103 final

Communication from the Commission, (2007), to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on creative content online in the Single Market, SEC(2007) 1710 COM/2007/0836 final

Communication from the Commission, (2009), Copyright in the Knowledge Economy, COM/2009/532 final

Council conclusions, (2008), 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 C 319

Geiger Cristophe, (2007), The role of the three-step test in the adaptation of Copyright law to the Information Society, E - Copyright Bulletin, online at: http://portal.unesco.org/culture/en/files/34481/11883823381test_trois_etapes_en.pdf/test_trois_etapes_en.pdf accessed 20.05.2010

Ginsburg Jane, (2001), Towards Supranational Copyright Law? The WTO Panel Decision and the Three Step Test for Copyright Exceptions, 187 RIDA 2, 14

Green Paper, (2008), Copyright in the Knowledge Economy, COM 2008, 466 Final

Griffiths, Jonathan, (2009), The three-step test in European Copyright Law, Problems and solutions, online at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1476968 accessed 20.05.2010

Harvard Education, (2009), Module 4: Rights, Exceptions, and Limitations, online at http://cyber.law.harvard.edu/copyrightforlibrarians/Module_4:_Rights,_Exceptions,_and_Limitations#Contributors, accessed 20.05.2010

Igglezakis Ioannis, (2002), "Web Hosting Agreement: Meaning, Function and legal nature", Trade Law Review, 8th year, Issue D, Oct. – Nov. – Dec. 2002

IVIR, (2007), Study on the implementation and effect in Member States laws of Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society, Final report, online at: http://www.ivir.nl/publications/guibault/Infosoc_report_2007.pdf, accessed 20.05.2010

*Infopaq International A/S v Danske Dagblades Forening,* Case C-5/08: Judgment of the Court (Fourth Chamber) of 16 July 2009 (Reference for a preliminary ruling from the Højesteret Denmark)

Koelman J. Kamiel, (2006), Fixing the Three-Step Test, EIPR, 2006/8, 407-412

Koren – Elkin Niva, (2009), Copyright and its Limits in the Age of User-generated content, Proceedings from the COUNTER Workshop Mashing Up Culture, Uppsala University, "Mashing Up Culture, The rise of User- Generated Content", May 13-14 2009, Sweden

Markellou Marina, (2009), From Copyright to Copyleft and from Copyleft to Copywrong or "If Hitler had Been a Hippy How Happy Would We Be" Evaluating the Practice of the Artistic Appropriation and its Legal Impact", Proceedings from the COUNTER Workshop Mashing Up Culture, Uppsala University, "Mashing Up Culture, The rise of User- Generated Content", May 13-14 2009, Sweden

Masouye Claude, (1971), Guide to the Berne Convention, WIPO

OECD, (2007), Working Party on the Information Economy participative Web: User – Created Content, on line at: http://www.oecd.org/dataoecd/57/14/38393115.pdf accessed 20.05.2010

Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, (2008) on Creative Content Online in the Single Market COM(2007) 836 final, OJ C 77

Phillips Jeremy, (2008), Just three steps but so many criteria, Editorial, JIPLP 2008, Vol. 3, No. 10

Regional Court of Hamburg, (2004) JurPC Web-Dok, 146/2004

Reynolds Graham, (2009), A stoke of Genius or Copyright infringement? Mashups and Copyright in Canada, SCRIPT-ed, (2009), 6: 3

Senftleben Martin, (2004), Copyright Limitations and the Three-Step Test, Kluwer Law International, 2004

Smith H. Eric, (2001), The reproduction right and temporary copies, The International Framework, the U.S. approach and practical implications, Paper presented to the SOFTIC Symposium, Tokyo, November 20-21, 2001

*Sociedad General de Autores v Editores de España (SGAE) v Rafael Hoteles SA*, (2006) Case C-306/05 [2006] ECR I-11519

Suzor Nicholas, (2005), Transformative Use of Copyright Material, online at http://nic.suzor.com/articles/TransformativeUse.pdf accessed 20.05.2010

Towse Ruth, (2003), Economics and Copyright Reform: aspects of the EC Directive, online at: www.recida.org/downloads/towse3.doc accessed 20.05.2010

United States – Section 110(5) of the US Copyright Act, (2000), Report of the Panel, WT/DS160/R

WIPO, (1997), The Implications of the TRIPS Agreement on WIPO Administered Treaties, WIPO/IP/PK/96/3, online at: http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=3296 accessed 20.05.2010

WIPO, (2000), Limitations and exceptions under the three-step test and national legislation, Differences between the analog and digital environments, WIPO/DA/MVD/00/4, online at: http://www.wipo.int/edocs/mdocs/copyright/en/wipo_da_mvd_00/wipo_da_mvd_00_4.pdf accessed 20.05.2010

WIPO, (2003), Copyright and Related Rights in the Context of the Internet, WIPO/IP/TIP/03/9, online at: www.wipo.int/arab/en/meetings/2003/ip_tip/doc/wipo_ip_tip_03_9.doc accessed 20.05.2010

WIPO, (2005), International Protection of Copyright and Related rights Document prepared by the International Bureau of WIPO, online at: http://www.wipo.int/copyright/en/activities/pdf/international_protection.pdf accessed 20.05.2010

WIPO, (2009), Understanding Copyright and Related Rights, online at http://www.wipo.int/freepublications/en/intproperty/909/wipo_pub_909.html#translation, accessed 20.05.2010

Wirten Hemmungs Eva, (2009), Prologue, Proceedings from the COUNTER Workshop Mashing Up Culture, Uppsala University, "Mashing Up Culture, The rise of User- Generated Content", May 13-14 2009, Sweden

## Endnotes

1. There is also no willingness to pay for such activities on behalf of the users. See in that regard Commission, (2009), Commission staff working document, accompanying document to the

Communication from the Commission, the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, SEC 2009, 1103 final.

2. However, in view of the purpose of the end – user to create a derivative work, the storage of the copyrighted work in question should take place rather in a permanent storage device than a temporary one. In any case, the permanent or temporary character of the storage device is not – in principle – the decisive factor for the act to be deemed as reproduction but rather a matter of whether there is a possible exception under copyright law. See in that regard Eric H. Smith, (2001), The reproduction right and temporary copies, The International Framework, the U.S. approach and practical implications, Paper presented to the SOFTIC Symposium, Tokyo, November 20-21, 2001. See generally Spinello Richard and Bottis Maria, A defense of intellectual property rights, 2009.
3. Directive 2001/29 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, OJ L 167.
4. Article 2 of the Directive.
5. Article 3 of the Directive.
6. Article 4 of the Directive.
7. *Infopaq International A/S v Danske Dagblades Forening,* (2009) Case C-5/08: Judgment of the Court (Fourth Chamber) of 16 July 2009.
8. See in that regard the reasoning of the Court in Recitals 44 - 51.
9. See Recitals 15,19 and 61 of the Directive.
10. Ibid.
11. *Sociedad General de Autores v Editores de España (SGAE) v Rafael Hoteles SA,* (2006) Case C-306/05 [2006] ECR I-11519.
12. At recital 43.
13. At recital 46.
14. We recall that even the act of obtaining a temporary copy infringes the reproduction right. Nevertheless, the act of obtaining a copy in the UGC context presupposes that such copy should be stored in a permanent storage device, so that the user will be able to interfere with it at any time in the future; that is why the analysis of the previous part focused on the receiving of the data (by downloading) and storing them on a permanent storage device (e.g. computer's hard disk).
15. See above at 2.1. as regards the recording of copyrighted sounds with a view to remixing.
16. The exception is mandatory, in the sense that Member States have to incorporate such an exception of copyright into their national legislation.
17. The list is exhaustive in the sense that member States may not adopt additional exceptions. See in that regard recital 32 of the Directive.
18. The exceptions are optional in the sense that member States are able to opt in adopting them in their national legislation or not.
19. The scope of the German "free use" rule appears, however, narrow. The Regional Court of Hamburg, in its "thumbnails decision", held that the reproduction of thumbnails on the Internet did not constitute a "free use" of the original image. The Court stated the reduction

of an image into a smaller thumbnail was an entirely automatic process that did not reflect any human activity. In addition, the reduction of an existing image to a "thumbnail" was not undertaken to create a new work but to create a smaller version of an image for the sole purpose of indexing and creating a link to the original. See Regional Court of Hamburg, (2004) JurPC Web-Dok, 146/2004.

20. *United States – Section 110(5) of the US Copyright Act*, (2000), WT/DS160/R.
21. Section 110 (5) A of the US Copyright Act (well known as the "homestyle" exemption).
22. Section 110 (5) B of the US Copyright Act (well known as the "business" exemption).
23. Report of the Panel, United States – Section 110 (5) of the U.S. Copyright Act, WT/DS160/R15, June 2000, at para. 6.74.
24. Report of the Panel, United States – Section 110 (5) of the U.S. Copyright Act, WT/DS160/R15, June 2000, at para. 6.112.
25. Report of the Panel, United States – Section 110 (5) of the U.S. Copyright Act, WT/DS160/R15, June 2000, at para. 6.163 – 6.219.
26. Report of the Panel, United States – Section 110 (5) of the U.S. Copyright Act, WT/DS160/R15, June 2000, at para. 6.173.
27. Report of the Panel, United States – Section 110 (5) of the U.S. Copyright Act, WT/DS160/R15, June 2000, at para. 6.220 – 6.272.

# The challenges of collective management in the digital era

**Evangelia Vagena**

## Introduction

The article aims at presenting a spherical and synoptic description of the conditions under which collective management of copyright and related rights is exercised in the digital era. A brief introduction on function of collective management seems necessary since the paper was originally prepared to be presented in a non legal audience. The impact of Digital Rights Management (hereinafter DRM) on collective management is then described. Clearing rights for online use is facilitated by the existence of one stop shops. Their expansion is one of the goals of the European policy in relation to the collective management. EU policy in this field has been made clear in the recommendation issued by the Commission in 2005. The recommendation is questioned especially because of its consequences for cultural diversity in the EU level. Collective societies are also very preoccupied by the difficulties of enforcement in the digital environment as well as by the open content licencing schemes which are more and more used. From the following analysis it becomes clear that collective management is absolutely necessary in order to ensure right holders receive their income and their rights are protected and therefore provide them with the incentive to continue creating.

## Collective management basics

The basic reason for the existence of collective management as an institution is the practical impossibility of individual control over the work by the author alone – the «author's incapability for self-protection» [Kotsiris, 2005].

While collective management is optional, in some cases it is compulsory. The Greek copyright legislation provides for three such cases:

a) the collection of private copying levies (Art.18 law 2121/1993)

b) the collection of the equitable remuneration ought to performers and the producers of the sound recordings used for a radio or television broadcast by any means, such as wireless waves, satellite or cable, or for communication to the public (Art. 49 par.1 law 2121/1993) and

c) in cases of unaltered and unabridged secondary transmissions of radio and television programs by cable or other physical means (Art. 54 par. 2 law 2121/1993).

Through the signature of reciprocal agreements among collecting societies of different countries an international net of collective management is created.

## The answer to the machine is the machine

The transition from the analogue to the digital environment led to the appearance of DRM. The prospect of revival of individual management with the help of DRM was soon refuted:

- individual management has a high cost;
- monitoring the works demands a special know-how from the individual author;
- Collective Management Organizations (hereinafter CMOs) dispose a strong bargaining power against the users of the work and they exercise political pressure for the defense of the author's rights while they constitute the contact point for authors and users [Vagena, 2010].

Taking into consideration all these facts, the prospect of individual management seems more realistic for the companies producing the works which may have the know-how as well as the money and the time to spend on the monitoring of the works.

The transition of collective management from the analogue to the digital environment was marked by the digital threats which transformed the convenience of collective management to a need. CMOs need to get modernized. They especially need to create electronic licensing platforms like ASPIDA, the online licensing platform recently presented by the Hellenic Collecting Society representing writers and authors (see at: http://aspida.osdel.gr/ERMS/). In this direction DRM are expected to enforce collective management in the digital environment.

## One-stop shops

The central management of rights in the digital environment takes the form of *one-stop shops*. One-stop shops are online services to which the users may be addressed for the clearing of all digital rights of a work. This way they avoid the time consuming transaction with all the right holders involved including different CMOs. They can be composed of all CMOs functioning under an umbrella and providing information and a single license for the use of each work. The danger of individualized negotiation for the licensing of each work exists. This is why the licensing of a work according to the tariff table of each CMO should be preserved in order to protect the works which are less commercially successful.

The need for adjustment of the traditional form of collective management is more intense in the EU where the users may need to ask for a license from 27 different CMOs for online use based on the member state where the work will be communicated. On the contrary in United States, the users need to ask for a license only from three CMOs (ASCAP, BMI, SESAC).

A series of EU funded projects for the creation of central rights clearance schemes for multimedia were realized in EU very early. They addressed:

- the networking of existing collectively managed multimedia rights clearance systems in six Member States (VERDI),
- the interoperability of digital content identification systems and rights metadata within multimedia e-commerce (INDECS),
- sector specific multimedia rights clearance systems for book publishing (EFRIS),
- audio-visual (TVFILES, PRISAM) and music (ORS) rights,
- the integration of electronic copyright management and multimedia rights clearance systems (BONAFIDE), and
- best clearance practices for educational multimedia (COMPAS) and protection of creative contributions in a collaborative networked multimedia title development environment (b©) [Gervais, 2006].

CMOs had already developed "one stop shop like" initiatives in the music sector before 2005. The "Simulcasting agreement" (2002) provided for pan-European licensing by any CMO in EU for simultaneous transmission by radio and TV stations via the Internet of sound recordings included in their broadcasts of radio and/or TV signals for simulcast of a work. The "Santiago agreement" (2000-2004) provided for multi territorial licensing from the CMO who functions at the country where the user has his official seat. The "Barcelona agreement" (2001-2004) was similar to the Santiago agreement but for mechanical rights. Nevertheless due to the European Commission's claims that these agreements were potentially in breach of European Union competition rules because they provided that the license could be asked for only by the CMO operating in the country the user had his official seat, the agreements were not renewed by the parties when they ended [Gillieron, 2006]

## EU policy on collective cross-border management of copyright and related rights for legitimate online music services

In 2005 the Commission Recommendation 2005/737/EC of 18 October 2005 on collective cross-border management of copyright and related rights for legitimate online music services was issued. According to its provisions member states should ensure that the right holders have the possibility to entrust the manage-

ment of any of the online rights (reproduction right, making available right, distribution right) on a territorial scope of their choice, to a collective rights manager of their choice, irrespective of the Member State of residence or the nationality of either the collective rights manager or the right-holder. They should also enjoy the right to withdraw any of the online rights and transfer the multi territorial management of those rights to another collective rights manager. The recommendation aimed to facilitate multi-territorial licensing for the online use of musical works.

The terms in reciprocal representation agreements were an obstacle to this direction until 2008. In particular, according to the territorial exclusivity clause users could only ask for a license regarding the repertoire of a foreign CMO from a national CMO. According to the membership clause a CMO could not accept as a member a right holder who was a member of another CMO. According to the European Commission decision of 16 July 2008 (CISAC decision) those clauses were found to be infringing rules on restrictive business practices (Article 81 of the EC Treaty and Article 53 of the EEA Agreement) concerning the exploitation of the works online, cable or satellite.

Following the recommendation of 2005, some new legal entities have appeared as non exclusive licensing agents of big music labels such as CELAS –Centralized European Licensing and Administrative Service which provides licenses for EMI music publishing's Anglo American repertoire for digital and mobile exploitation across Europe, (see at www.celas.eu). Also agreements have been signed between big music publishers and CMOs, so that the last ones operate as non exclusive licensing agents of the repertoire of the publishers, see for example the Pan-European Digital Licensing initiative (PEDL) for the repertoire of the Warner Company in cooperation with five CMOs.

The criticism of the 2005 recommendation refers to the consequences for the preservation of cultural diversity because of the "monopolistic" concentration of the rights management by the strongest CMOs which administer the more commercial part of the universal music repertoire (the Anglo-American). This criticism is expressed not only by the weakest CMOs but also by the European Parliament itself (see for example the European Parliament resolution of 13 March 2007). It is claimed that it constitutes a threat for the small and medium sized CMOs from the concentration and control of the rights by the biggest CMOs. A question which rises in this context is whether competition among CMOs will benefit culture more than solidarity. European policy should promote both elements so that collecting societies spent more time and energy in collaborating in order to face the common threats appearing in the digital era than in competing each other in order to survive as legal entities.

A very interesting study was prepared by the Hellenic Foundation for European and Foreign Policy (ELIAMEP) in June 2009 concerning the collecting societies and cultural diversity in the music sector. Its basic findings were the following. The new licensing channels that have been established for the provision of EU-wide licences concern specific types of repertoire, primarily the Anglo-American repertoire. Most of the business models which have emerged in this direction have derived from major music publishers which have withdrawn the management of the mechanical rights of the most commercial part of their repertoire from the system of reciprocal representation in relation to digital licensing. Such rights have been entrusted to specific collecting societies or newly created collective rights management bodies for pan-European digital exploitation. Major publishers will continue to use the system of reciprocal representation through national CMOs for other rights influencing this way the function of CMOs especially by threatening that they will withdraw the management of the rest of their rights.

In the framework of the Online Commerce Roundtable set up by Commissioner Neelie Kroes, some general principles on the online distribution of the work were adopted. They were expressed in a Joint statement from the Online Commerce Roundtable participants on "General principles for the online distribution of music" issued on 20.10.2009. The roundtable was composed of CMOs, producers, consumer unions, representatives of the IT sector. They all agreed to pursue the development of efficient licensing platforms offering pan-European/multi-territorial licences for the performing (public performance) and the mechanical (recording and reproduction) rights to commercial users. According to the statement such platforms should be non-exclusive and non-mandatory. The issues remaining to be solved as described in the statement are: a) the need to develop standardized rights management information so that interoperability & interconnection of the existing data bases is achieved (a special working group was set up), and b) the need to find a transparent and non discriminatory way of choosing the legal entities which will undertake the licencing of the online rights.

## Enforcement in the digital environment

Collecting societies are also very preoccupied by the issue of the enforcement of copyright in the digital environment. They have developed surveillance systems in order to monitor illegal sites and file sharing. They often communicate directly with the website owners when a publication on their sites is infringing copyright. If the website owners refuse to withdraw the infringing publication, they communicate with the ISP (internet service provider) asking him to prevent access to the infringing content. The need to co-operate with ISPs was underlined in the memorandum of understanding which was signed between right holders representatives and representatives of the telecommunications' sector in France

in 2004. In other policy reports it is also generally admitted that it would be especially useful to develop notice & take down systems following the example of the American Digital Millennium Copyright Act (DMCA).

Copyright enforcement is especially difficult in relation to P2P file sharing systems. Users who share files can only be identified by the IP address the computer they use is receiving at the moment of the exchange of the infringing content. The IP address is covered by the protection of personal data and the protection of secrecy of communications. There have been many legal discussions and some court decisions on whether or not the users' real identity should be revealed to the right holders in order to defend their rights.

CMOs are in general reluctant regarding aggressive actions against end users. Still, they support the graduated response system otherwise called 3 strike test: According to this system the first step is to contact the ISP, to inform him about the suspected actions taking place through his services by a user identified by his IP address so that the ISP contacts him through email and warns him about the consequences of his actions. If another suspicious action takes place through the same IP address, a certified letter is sent to its owner with the same warnings. If the owner of this address does not comply or if he/she is again accused of repeating these offenses, then the ISP suspends the internet service for the internet connection, the object of the claim, for a period given. This system has been already adopted by the French law HADOPI and has been included in the British bill for Digital Economy.

A possible solution widely discussed for the issue of P2P would be the adoption of a form of compulsory license for the use of a work on internet. In France this solution was promulgated in the scheme of "*licence globale*" in order to make the non commercial peer-to-peer exchanges of audiovisual content legal in exchange for a fee on broadband Internet subscriptions. This fee would be proportionate to the actual online use of a work and would be distributed to the artists and authors. The major objection to all similar proposals is that they transform authors' exclusive rights to simple claims for damages depriving them from the absolute character of their rights. Still, since these rights are not effectively enforced in the digital environment, the question whether a bad solution could be better than a worse one remains.

Other forms of illegal file sharing also exist apart from P2P exchanges. Protected content could be shared without authorization from the right holders through instant messages, like email or sms messages or thought e- readers, like IpoD or MP3 players. Characteristic examples are included in an interesting survey of the Pew Internet & American Life Project (see at http://www.pewinternet.org/Reports/2005/Music-and-Video-Downloading.aspx). In these cases "licence

globale" could not offer a solution. The only way to limit the extent of this unauthorized use of works would be the use of suitable technical measures of protection.

## Open content movements

At the same time CMOs are trying to control the use of their works with more restrictive measures, they are also trying to adapt themselves to the reality of open content movements. The most characteristic of these movements is the Creative Commons (CC) movement. Creative commons licenses are based on the combination of four basic elements of the licenses, from which one, the credit to the original author, remains common in all the alternative forms of CC licenses. The four basic elements of the Creative Commons licenses are:

a) the credit to the original author of the work (attribution),

b) the distribution of derivative works only under a license identical to the license that governs the initial work (share-alike),

c) the prohibition of making derivative works (Non Derivatives) and

d) the prohibition of the commercial use of the works (non Commercial).

If the right holder wants to license some of the works under creative commons licenses, although he has assigned the administration of his rights to a CMO, he cannot. The assignment contract covers all the existing works but also the future ones, usually for a period of no more than 3 years (term of duration of the assignment contract). Some efforts to compromise the logic of CC licenses and the provisions of the assignment contract have been made [Kapellakou, Markellou, Vagena, 2010]. The first one was Buma/Stemra which agreed with Creative Commons of Netherlands to start a pilot allowing its members to make their musical works available under non-commercial Creative Commons licenses. Composers and lyricists who until now released their work exclusively under Creative Commons licenses can also choose to become members of Buma/Stemra, enabling that organization to collect the remunerations for commercial use of their work. This pilot is considered to bring to an end the "all-or-nothing" scenario regarding the repertoire of an author. Following Buma's example KODA, the Danish Authors' Society, has also started offering noncommercial Creative Commons licensing to its members – making it the second country worldwide to do so. Members must sign an agreement with the KODA in which they indicate which works they wish to license, and for the purpose of this arrangement, only Creative Commons licenses with the "non commercial" condition can be used. More recently STIM, the Swedish Performing Rights Society, started offering its members the opportunity to sign a so-called Creative Commons license (CC) for a trial two-year period. The license enables creators to release individual works for non-commercial use.

The role of CMOs in the digital environment seems to become more demanding. One may question the way of functioning of some CMOs. Still, it has been proven that in any case of mass use of the use of works (like in internet) collective management is the only system which can guarantee for right holders the payment they deserve and thereof the necessary motive and means for cultural creativity. Collective management will be unavoidably altered but hopefully not substantively.

## References

Gervais D. (ed.), Collective Management of Copyright and Related Rights, Kluwer Law International, 2006

Gilleron Ph., Collecting Societies and the digital environment, IIC 2006, p.939

Hellenic Foundation for European and Foreign Policy, Collecting Societies and cultural diversity in the music sector, study for the EU Parliament, Directorate General for Internal Policies, 2009

Kappelakou G., Markellou M. and Vagena E., Open content in libraries-contractual issues, to be published in the book E-Publishing And Digital Libraries: Legal and Organizational Issues by Igglezakis I., (ed.), Synodinou T.E (ed.), Kapidakis S.(ed.), IGI Global publishing, 2010

Kotsiris L., Copyright law (in Greek), Sakkoulas, 2005.

Vagena E, The technological protection and digital management of Copyright, Thesis, Law School, University of Athens, 2010 (in Greek-unpublished).

# Setting new limits to the protection of digital media

**Petroula Vantsiouri**

## 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, which are designed to prevent acts of exploitation of intellectual property rights by way of controlling copying or access to works.[1] As 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 rightholders concerned specific protection when trying to enforce and manage their rights by technical means. These so-called anticircumvention 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. [2]

At a global level the protection against circumvention of TPMs is recognized in the WIPO Copyright Treaty (hereinafter WCT) and in the WIPO Performances and Phonograms Treaty (hereinafter WPPT). The WCT and the WPPT, the so-called WIPO Internet Treaties, oblige the contracting parties to provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors, performers or producers of phonograms in connection with the exercise of their rights and that restrict acts, in respect of their works, which are not authorized by the right holders concerned or permitted by law. The anticircumvention rules were implemented in the EU and the US in the European Directive 2001/29/EC of the European Parliament and of the Council of May 22, 2001 on the harmonization of certain aspects of copyright and related rights in the information society (Information Society Directive) and in the Digital Millennium Copyright Act (DMCA) respectively. Article 6 of the Information Society Directive requires that Member States must provide adequate legal protection against circumvention of TPMs, whereas the Section 1201 of the DMCA prohibits the circumvention of effective access controls as well as the trafficking in circumvention tools of effective access and copy controls.

TPMs were hailed by the copyright industries as effective enforcement mechanisms that would protect their interests from the risks of piracy in the digital

and networked environment and as means to enable them to take advantage of the new possibilities that the advent of technology provided them. Supporters of TPMs claimed that copyright works made available in digital formats would be especially vulnerable to unauthorized copying and redistribution and thus copyright holders would be discouraged to make their works digitally available to the general public.[3] On the other hand, critics of TPMs claimed that introduction of technological measures and their protection by anticircumvention laws would restrict access to works in the public domain and that they would not respect traditional copyright exceptions.[4]

The question of whether the legislature came to the right solution when enacting anticircumvention provisions remains one of the hottest ones on the agenda. However, anticircumvention regulation raises a variety of legal issues not only within the scope of copyright law but also in neighbouring domains, which have not attracted the same attention. One of these issues concerns the misapplication of anticircumvention laws to restrict healthy competition in aftermarket products markets. In particular, manufacturers and vendors of consumer primary products may seek to prevent competitors from selling replacement parts or other compatible parts (aftermarket products), by using some kind of TPMs in the primary products or the aftermarket products. The manufacturers then could try to use the anticircumvention clauses to prevent competitors from distributing products, which circumvent the TPMs. More specifically, vendors and manufacturers of consumer primary products, who hold a dominant position in the primary product market, can use anticircumvention regulation in order to reinforce their dominant market position in the aftermarket by preventing interoperability of products on alternative systems.

The notorious Lexmark International, Inc. v. Static Control Components, Inc case (387 F. 3rd 522, 2004) which involved a printer manufacturer trying to prevent others from remanufacturing printer cartridges, presents an excellent example that indicates how a company may seek to benefit from the protection granted by anticircumvention provisions for advancing its own monopoly position and for hindering competition in the aftermarket. Lexmark's behaviour, though, was not unprecedented in the market for printers. Printer prices are increasingly subsidised by cartridge sales, as the combination of cheap printers and expensive cartridges enables vendors to target high-volume business users and price-sensitive home users with the same products.[5] However, the availability of reeled cartridges, and cartridges from third-party aftermarket vendors limit the level of cross-subsidy and thus TPMs have been employed in order to eliminate competition in the aftermarket. Similar business models have been applied in the adjacent markets for consoles for computer games and computer games, in the markets for

mobile phones and service providers for mobile phones and recently in the markets for smartphones and applications for smartphones.[6]

In general, the practical issues as designated by US and European jurisprudence indicate that the anticircumvention provisions give birth to competition law issues that do not arise from the classic interaction between Intellectual Property and Competition. Intellectual Property rights create a temporary monopoly for their right holders, for which the legislator has set certain restraints so that the exercise of those rights does not obstruct healthy competition. According to supporters of TPMs the rationale behind the adoption of anticircumvention regulation is to enforce this monopoly and fulfil the goals of Intellectual Property legislation. However, anticircumvention legislation can result into creating further monopolies, which the legislator initially did not aim to protect and are not subject to the restraints imposed on Intellectual Property rights. Thus, the question that arises is how to balance the conflicting objectives of Intellectual Property and competition law and decide whether Intellectual Property protection should be enforced by extending monopolies to further markets in expense of competition in these secondary markets or whether healthy competition should prevail over the interests and the incentives for the authors of creative works.

This paper analyses the impact of the anticircumvention provisions of the Information Society Directive and of the DMCA on healthy competition and in particular it addresses their misapplication for advancing the monopoly position of copyright holders. It argues that judicial interpretation of the EU and US anticircumvention legislation does not have the flexibility to balance the risks of tolerating piracy with fragmenting the market and that competition law is not capable of restoring this balance. Thus, it calls for an amendment of the existing legislation at an EU level as well as in the US. Parts 2 and 3 of this paper outline the substantive provisions of the Information Society Directive and the DMCA and examine how their application has led to anticompetitive conduct, being challenged in the courts. Part 4 analyses the inability of competition law to restore the anticompetitive effects generated by the misuse of the anticircumvention regulation. Finally Part 5 addresses the need for amendment of anticircumvention laws and attempts to propose how the doctrine should be amended in order for a better balance between protecting the legitimate rights of copyright uses and safeguarding competition in the market to be achieved. In particular it suggests, firstly, that the infringement of the anticircumvention norms should be explicitly conditioned to the infringement of a valid copyright and secondly, that there should be no differentiation in the treatment of tangible articles of commerce and cultural artifacts and courts should be instructed to apply all exceptions equally to both categories of works.

## The substantive provisions on anticircumvention

### *The Information Society Directive*

Article 6 of the Information Society Directive explicitly requires Member States to provide adequate legal protection against circumvention of effective technological measures[7] designed to prevent or restrict acts not authorized by the copyright holder, including the trafficking in devices, products or services which may be used to circumvent such technology.[8] As regards the implementation of the Information Society Directive by Member States, the Directive's open wording has led to significant differences among implementing laws.[9] This has led to continuing controversies over the Directive itself and conflicts about the appropriate design of copyright law for the digital age. Unlike the DMCA, the Information Society Directive does not treat access and copy controls differently, as the definition of TPMs in the Directive indicates. [10] Furthermore, whether the act of circumvention actually infringes a copyright is not relevant for the purposes of the protection of the TPM.[11]

Article 6(4) of the Information Society Directive regulates permissible exceptions to strict TPM protection.[12] In other words, Article 6(4) regulates the occasions when the beneficiaries of certain copyright exceptions provided in Article 5 of the Directive are hindered from making use of these exceptions due to the TPMs. However, TPMs enjoy legal protection also when they hinder the beneficiaries of the exceptions of copyright from benefiting from them, as they are not exceptions to the liability of the circumvention of technological measures.[13] On the contrary, the Directive sets out a unique legislative mechanism, which imposes an ultimate responsibility on the right holders to accommodate certain exceptions.[14] In particular, the exceptions are reinforced voluntarily by measures taken by the right-holders and, if the right holders do not comply with this obligation, Members States must ensure that right holders provide beneficiaries of the exceptions with the appropriate means to benefit from them.[15]

While the Directive has a broad, but closed list for exceptions for fair dealing, the exceptions applicable to TPMs are limited. In particular, Article 6(4) sets out two categories of exceptions: the home copying exception, which is optional; and the public policy exceptions, which are mandated. The public policy exceptions are the photocopying exception, the archival copying exception, the broadcaster's exception, the non-commercial broadcast exception, the teaching and research exception, the disability exception and the government exception.

From the exceptions contained in the Directive, only the research exception could exempt from liability a competitor who circumvents a TPM in order to manufacture and/or distribute interoperable products with the product that incorpo-

rates the TPM. Relevantly, however, this exception is subject to a condition: it is available only to the extent "justified by a non-commercial purpose" and the circumvention's sole purpose must be that of scientific research. Thus, the 'research exception' cannot be relied on as defence by competitors who try to enter a market closed by TPMs. Notably the exceptions in the Information Society Directive also do not include "reverse engineering". Such an exception exists in the Directive 91/250/ECC of 14 May 1991 on the legal protection of computer programs (Software Directive), which provides a limited safe harbour for those trying to achieve software interoperability.

It has been argued that Member States' ability to enact exceptions with regards to the protection of TPMs is limited to those enumerated in the list in articles 6(4) subparagraph (a), as there is no other reason for these exceptions to be specially picked out.[16] Such an approach, however, may disregard Recital 48 of the Information Society Directive, which requires that legal protection against technological measures should not hinder cryptographic research, although the Directive itself does not contain such an exception. In the end, and as the Recitals are not legally binding, it would be up to the ECJ to decide whether the Member States' implementing laws are in compliance with EU law, although such a controversy has not appeared in practice. In any case, the limited number of exceptions to the protection of TPMs that are provided in the Directive takes away from the Member States the flexibility to respond to changing technological situations and to respond to issues such as the anticompetitive use of the TPMs to raise barriers of entry to adjacent markets.

More importantly, the EU legislator nullified the exceptions to copyright in two ways: First, since general exceptions permitted by Article 6 do not automatically apply with respect to TPMs, copyright holders can impede TPMs in their works, so that the beneficiaries of the exceptions can not enjoin them. Secondly, even if one of the exceptions to Article 5 also applies with regard to TPMs, the beneficiaries can not make use of the exception contrary to the will of the copyright holder, unless they participate actively in judicial proceedings.

To elaborate further, the list of exceptions applicable with regard to copyright works protected by TPMs is limited, especially as seen by comparing it to the broad list of exceptions in Article 5 of the Information Society Directive.[17] Thus, the exceptions to copyright in Member States differ depending on whether a particular work is protected by TPMs or not. Accordingly, the exceptions which do not apply with respect to TPMs can be easily overridden by the copyright holders by simply impeding a TPM. To illustrate that, if a Member State has enacted an exception permitting reproduction of a work by the press without liability,

as permitted under Article 5(3)(c) of the Information Society Directive, it must punish the reproduction if it is obtained by circumventing a TPM.

Furthermore, the move away from the traditional norm where the exceptions are positive rights to use and the enactment instead of a unique legislative mechanism, which foresees an ultimate responsibility on the right holders to accommodate certain exceptions, places the burden of reassuring the application of those exceptions from the state to the beneficiaries of the exceptions. Practically, the beneficiaries of an exception will not be able to enjoy a copyright work if the copyright holder has not voluntarily agreed to do so and they will not be entitled to circumvent the TPMs either; instead they should engage into a timely and costly judicial proceeding against the particular right holder to be able to benefit from the exception. Of course, other copyright holders may still not permit the exception.

Summing up, there are three main problems with the anticircumvention provisions of the Information Society Directive. Firstly TPMs are protected also when they do not prevent copyright infringement; secondly, the number of exceptions applicable to TPMs is limited and in particular there is a lack of a reverse engineering exception; thirdly, the exceptions provided in Article 6 para 4 of the Information Society Directive are not exceptions to the liability of the circumvention of TPMs.

### *The DMCA substantive provisions on anticircumvention*

The DMCA protects both access controls[18] and copy controls.[19] Both the act of circumvention[20] and trafficking in circumvention technologies are prohibited for the first; for the second, only trafficking in technologies that circumvent copy controls is banned. The DMCA created three new causes of action: Section 1201(a)(1)(A) prohibits the circumvention of TPMs that control access to copyright works; Section 1201(a)(2) prohibits -- under specific conditions -- making, offering to the public, or otherwise trafficking technology that circumvents TPMs that control access to the work; and, likewise, Section 1201(b)(1) prohibits – also under specific conditions -- making, offering to the public, or otherwise trafficking technology that circumvents TPMs that control specific uses of the work.[21]

Still, the statute exempts certain activities from one or all of the causes of action recognized in Section 1201. These exemptions are either expressed in the statute itself or have been recognized by the Library of Congress, pursuant to a congressional mandate in Section 1201(a)(1)(c).[22] One of those exceptions is contained in Section 1201(f). This exception specifically allows reverse engineering of TPMs that protect computer programs in order to obtain interoperability.[23]

The interoperability exception allows the circumvention of TPMs that effectively control access to a particular portion of a computer program under the conditions that the circumventor has lawfully obtained the right to use a copy of that program and circumvention occurs for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently-created computer program. Additionally, the information obtained through reverse engineering should not be readily available to the person engaging in the circumvention and the identification and analysis should not constitute infringement.[24] The circumventor may make available the information that she obtained by the permitted circumvention, if she provides such information solely for the purpose of enabling interoperability to the extent that the actions do not constitute infringement.[25] The law provides an opportunity to distribute solutions to the interoperability problems to users with minimal technical knowledge, who would not have been able to circumvent the TPMs themselves; however it premises this safe harbor under the aforementioned narrow conditions.

The statute's main flaws include that it fails to protect against the circumvention of TPMs protecting copyright works other than computer programs and that it does not protect data interoperability.[26] In short, the interoperability exception does not deter companies from employing TPMs to restrict the development, distribution and use of interoperable technologies. Thus, despite of the inclusion of Section 1201(f) (1) and (3), the DMCA discourages the creation of unauthorized interoperable products; it prohibits their distribution and exposes the users of technologies that enable interoperability to liability.

Having examined the flaws of the EU and US anticircumvention provisions, it should be further examined whether those problems can be alleviated via the judicial route or whether there is a need for amendment of the anticircumvention norms. There are quite a few examples from the jurisprudence on the Information Society Directive and on the DMCA on that demonstrate how companies have tried to benefit from anticircumvention regulation in order to establish themselves in secondary markets. These cases also provide guidance on how one can expect the courts to handle future anticircumvention cases.

## Relevant case law

### *Jurisprudence of European Courts*

Neither the Court of First Instance nor the European Court of Justice ECJ have yet had the chance to interpret the substance of the provisions of the Information Society Directive regarding TPMs.[27] Thus, for the time being, one has to rely on the interpretations of the implemented provisions of the Directive by the national courts

of the EU Member States. Even narrowed thus, the pool of interpretations is quite small – since many Member States delayed in implementing the Directive.[28]

Of particular interest is a dispute initiated by Kabushiki Kaisha Sony Computer Entertainment before the Tribunale di Bolzano, in Italy against Dalvit Oscar, a vendor of "neo 4" mod chips used to evade the protection measures of Sony's PlayStation (Defendant). The case demonstrates the efforts of the courts to interpret the Italian law implementing the Directive in a way that balances the goals of defeating piracy,[29] safeguarding healthy competition in the market and promoting consumer welfare.[30]

However, this is not the only interesting feature of the decision. Also of note is the fact that it involves efforts by a major computer game manufacturer, Sony, to control the market for its games.[31] Computer games manufacturers have been attempting to manipulate barriers to entry for many years. The business strategy that they follow is to subsidize sales of the actual consoles with sales of cartridges or, more recently, CDs containing the software. Sales of accessories, such as memory cards, are also controlled. [32] This was one of the many lawsuits that Sony initiated on globally invoking the anticircumvention legislation against unlicensed accessory vendors.[33]

The Defendant was selling the "neo 4" mod chips. These chips evaded the TPMs in the PlayStation2 console, so that the console could read pirated discs. This also meant that the console could read original Sony disks imported from countries with different region codes to the console; [34] disks containing games produced by other companies; back-up copies of original Sony discs; as well as disks containing programs other than games, so that the console could be used as a personal computer. The Defendant advertised the aforementioned mod chips in the site "hardstore.com".

The proceedings followed the seizure of modified consoles, mod chips, and related material, initiated by Sony, who later joined the penal proceedings as civil party (Party Civile). The seizure was based on Article 171ter (f) bis of the law on author's rights (Lda)[35], which implemented Article 6(2) of the Information Society Directive in Italian law.

Article 171ter (f) bis Lda provides that "it is an offence to make, import, distribute, sell, rent, transfer in any other way, advertise for sale or rental, possess for commercial purposes devices, products, or components or offer services which have as their predominant purpose or commercial use to avoid effective technical protection measures or which are principally designed, produced, adapted, or put into effect for the purpose of making possible or facilitating the avoidance of such measures" [emphasis added].

The Defendant responded that Article 171ter (f) bis Lda did not apply because the PlayStation2 Console was a "computer" and the games played were "computer programs"; thus, Article 171bis should apply instead. The nature of computer games as programs is crucial, because under Article 171bis, which implemented the Software Directive, liability can be established only if the sole function of the infringing device is to overcome the TPMs protecting the computer program. In contrast, under Article 171ter, which implemented the Information Society Directive and applies to TPMs protecting copyright works other than computer programs, a device infringes the law if its main purpose is to overcome TPMs.

Furthermore, the Defendant argued that, even if Article 171ter were to apply, the "predominant purpose or commercial use to avoid TPMs" requirement of the provision would not be satisfied, as the main function of the mod chip was to overcome monopolistic obstacles and to make better use of the console. Moreover, the Defendant claimed that according to the correct interpretation of Article 102quarter Lda, the protection of TPMs applies only if the function of the TPMs is to prevent copyright infringement and since Sony's TPMs did not serve this purpose, they should not enjoy legal protection.[36] Finally, it claimed that the contractual conditions limiting use contained within the packaging of the console were ineffective as all the terms of the contract must be known or knowable to the purchaser at the time of the formation of the contract for sale.

The proceedings followed the seizure of modified consoles, mod chips, and related material. An interlocutory decision was issued upholding the Defendant's arguments; but, when the case was tried, the First Instance Court found in favour of Sony. This decision was appealed and reversed by the Court of Appeals. Finally, the case reached the Supreme Court of Italy.

The Sezione per il riesame, in its interlocutory decision of December 31, 2003 found in favour of the Defendant in an effort to protect competition in the market for video games and to advance consumer welfare and consumer choice.[37] The Court held that circumventing effective TPMs was not the main use of the mod chips, because the devices also had other legal uses. The Court also noted that the Defendant had not violated the Italian anticircumvention law, because its acts did not violate Sony's copyrights. Finally, the Court also held that there was no apparent reason why the purchaser of a console should be restricted as to its use through Sony's protection measures[38] and that the contractual terms that Sony imposed on its users were ineffective.

The First Instance Court found Article 171ter (f) bis applicable. It did so by holding that the console was not a "computer" and that the video games were not "programs". This was because they involve images, sounds and text. Since computer games should be appropriately regarded as copyright works, to which TPMs

can be attached, the Court concluded that the defendant's behaviour should be assessed under Article 171ter.[39] Furthermore, the court held that protection of TPMs is offered independently of whether they protect author's rights, quoting directly from Art. 102.[40] Finally, the court held that the "predominant purpose to circumvent" requirement of Article 171ter (f)bis was satisfied. The Court accepted that Article 171ter envisages possible legitimate uses for devices, which also have the effect of overcoming TPMs and it rejected as illegitimate all the alternative uses suggested by the defendant.[41]

The Court of Appeals was more receptive to the defendant's arguments.[42] The Court held the PlayStation2 console to be a computer and the programs played on it to be computer programs. This meant that Article 171ter applied. That provision required proof that the only purpose of the mod chip was to overcome TPMs. That condition was not satisfied in this case because reading the back-up copy was permitted under Italian law. The Court further held that only the TPMs, which protected the author's rights, were protected.

The Corte di Cassazione in the decision 3368/2007 of the Terza Sezione reversed the Court of Appeal's decision.[43] The Supreme Court held that Sony's video games were not software programs, since the definition provided in Article 171 ter (d) better suited them. Thus, in order for the defendant to be found guilty, Sony only needed to prove the lower standard: that the mod chips' primary use was to overcome its TPMs.

Further, the Supreme Court overruled the Court of Appeal's finding that TPMs are protected only when they prevent copyright infringement and establish a right of access. The Supreme Court emphasized that article 102 of law 633/1941 had to be interpreted so as to protect the entirety of TPMs, including those in 171ter (F) which covered all TPMs designed to prevent acts that are not authorized by the copyright holder.

Courts in Italy have followed the Supreme Court decision. This is demonstrated by a recent decision of the Tribunale di Milano.[44] Following the same reasoning as the Supreme Court, the industrial and intellectual property division of the Tribunale ordered the seizure of mod chips, available from PCBox on the grounds that they violated the TPMs of Nintendo. The judge held that, since the primary function of the Mod chip is to read games that are copied, the chips should be confiscated.

Both the interlocutory decision as well as the decision of the Court of Appeals tried to provide an interpretation that would favour healthy competition in the market for video games and would advance consumer welfare and consumer choice. However, the Supreme Court held such an interpretation deviates from

the spirit of the Information Society Directive. Although it may seem desirable that, in cases of extreme abuse of anticircumvention regulations by copyright holders, the European Courts should find in favour of healthy competition, the existing legal framework and judicial precedent create the wrong incentives. They do so by deterring competitors from engaging in practices that would enable them to enter into a market but risk liability under anticircumvention law.

### *Jurisprudence on the DMCA anticircumvention provisions*

There is a common understanding among the critics of the DMCA that early litigation interpreting the statute expanded the definition of TPMs to such an extent that even modest innovations that could not qualify for patent protection would receive patent-like protection through anticircumvention laws.[45] However, it has been claimed that subsequent judicial interpretation has alleviated these dangers, and that the courts have struck the right balance between innovator's interests and permitting public access and enhancing overall social welfare.[46] It will be demonstrated that, even after these new decisions, which seem to recognize some of the negative consequences of an overbroad application of the DMCA, the existing law can still discourage innovation and limit competition in the market.

### *Sony Computer Entertainment America, Inc. v. Gamemasters*

One of the first cases to interpret the DMCA was Sony Computer Entertainment America, Inc. v. Gamemasters.[47] The video game manufacturer, Sony, sued Gamemasters for violating the DMCA. Gamemasters were selling a technology, called "Game Enhancer" that enabled players to modify Sony's Playstation. The court held that Game Enhancer violated the DMCA because its primary function was to circumvent a TPM, in particular the console's territory code mechanism. The court further held that the plaintiffs did not need to show copyright infringement.[48] Thus, although protection against piracy was not an issue in this case - which is the main objective that the DMCA is supposed to serve - the Court acknowledged that Sony had a right, broader than the rights conferred by copyright law, to control the uses of its work. The effect of that right was to permit Sony to restrict the development of new technologies.

### *Universal Studios v. Reimerdes*

Universal Studios v. Reimerdes[49] is another important case shaping the interpretation of the DMCA, as the District Court offered expansive readings of the DMCA's liability provisions and narrow interpretations of its various defences. Motion picture studios brought action under the DMCA to enjoin an Internet web-site owner, Corley, from posting for downloading computer software

that decrypted digitally encrypted movies on DVDs and from including hyperlinks to other web-sites that made decryption software available.[50]

The District Court held that DVD-copying programs violated the DMCA, despite the fact that they may have legitimate end uses and it enjoined their manufacture and sale.[51] Furthermore, it held that a technology can be found illegal independently under the Section 1201 of the DMCA, regardless of whether copyright infringement occurs.[52] As regards the interpretation of the interoperability exception, the District Court found Section 1201(f) inapplicable, as the provisions applies only to the circumvention of TPMs that restrict the access to computer programs, not copyright works generally.[53] The Court further heightened the "sole" purpose for achieving interoperability requirement of the Section 1201(f)[54] and it, additionally, found the public distribution of exempted tools and information under Section 1201(f) unlawful. As Reimerdes offered the sole judicial analysis of the interoperability exception until Davidson[55] was decided in 2004, the court's reasoning when rejecting the Section 1201(f) defence is of great interest.[56]

Rejecting the interoperability exemption on the basis that CSS[57] restricted access to movies stored on DVDs, is fully supported by the text of the provision that permits the circumvention of TPMs to "a person who has lawfully obtained the right to use a copy of a computer program" (emphasis added).[58] However, heightening the sole purpose requirement of Section 1201(f) and limiting the distribution of interoperability information and circumvention tools indicated scepticism from the court towards the statutory exception. To elaborate, the court held that the sole purpose requirement demands the plaintiff to show that interoperability is necessary to access or use a work, without baring the burden of actually proving the purpose of development of the circumventing device. [59] Second, the court ignored the language of Section 1201(f)(3) and held that the statute permitted dissemination of information obtained through reverse engineering, but not the means of circumvention used to obtain such information.[60] Finally, the court erred in imposing a blanket rule against the public distribution of exempted tools and information, despite the fact that DMCA contains no freestanding limit on the scope of distribution. More specifically, the court claimed that DMCA permits the sharing of interoperability information only by one who acquires that information. Such an interpretation, though, prevents publication of interoperability tools and information for a variety of purposes, including academic research.[61]

Although Section 1201(f) premises the safe harbour of the interoperability exception under really narrow requirements, the District Court's interpreta-

tion in Reimerdes raised the bar for the applicability of those requirements even higher. The combination of the narrow requirements of Section 1201(f) and their judicial interpretation in favour of copyright holders has nullified the importance of the statutory exception. The fact that no defendant has yet succeeded in a Section 1201(f) defence supports this argument. Thus, the interoperability exception failed to deter copyright holders from employing TPMs to restrict the development, distribution and use of interoperable technologies; on the contrary the judicial interpretation of Section 1201(f) in Reimerdes emboldened plaintiffs to test the bounds of their control over interoperable products.[62] Lexmark's, Chamberlain's and Storage Technology's attempts to increase their market power by employing TPMs were the result of the early judicial reading of DMCA as demonstrated above.

### *Lexmark Int'l, Inc. v. Static Control Components*

In Lexmark Int'l, Inc. v. Static Control Components[63], a major manufacturer of laser and inkjet printers who was also active in the market for cartridges for printers, attempted to enjoin its competitor, Static Control Components (SCC), from providing consumers with cartridges for the Lexmark printers by invoking the DMCA. Lexmark sold prebate cartridges at a deep discount in exchange for an agreement that consumers would use the cartridge only once and it employed a TPM intended to prevent unauthorized cartridges from interoperating with its printers.[64] Defendant, SCC, had created the SMARTEK chip, which mimicked Lexmark's authentication sequence and could bypass Lexmark's TPM. Lexmark alleged that SCC was trafficking in a circumvention device,[65] and sought to enjoin it from selling cartridges with SMARTEK chip. The District Court granted Landmark's request for a preliminary injunction,[66] but the Sixth Circuit reversed. The court held that access to the Lexmark's copyright software wasn't controlled by the authentication sequence, but by the purchase of a Lexmark printer because the authentication sequence wasn't encrypted or otherwise protected against literal copying.[67] Since the authentication sequence did not meaningfully control access to the code, the DMCA did not apply.[68]

Although Lexmark narrowed the scope of the DMCA by conditioning its application upon the robust protection of the copyright work by TPMs[69], it could allow future plaintiffs to succeed under slightly different facts, if they ensure that their TPM is effective.[70] Likewise, both Chamberlain Group, Inc., v. Skylink Techs [71] and Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc. [72] narrowed the scope of the DMCA, this time by requiring a nexus between the access facilitated by the TPM and the protection of a legitimate copyright interest. However, the courts did not offer enough guidance

as to the factual and legal predicates necessary for liability under the nexus requirement.[73]

### *Chamberlain Group, Inc., v. Skylink Techs*

Chamberlain, a Garage door opener (GDO) manufacturer, sued Skylink, a manufacturer of universal remote transmitters for patent infringement and violation of DMCA. Chamberlain alleged that the rolling code used in its GDOs protected access to the copyright code that operated the GDOs and that Skylink transmitters permitted unauthorized access to the software that operated Chamberlain's GDOs, by imitating the rolling code. The United States District Court for the Northern District of Illinois entered summary judgement in favour of defendant on the DMCA claim, holding that consumers who purchased Chamberlain products were entitled to access the GDO software, and Chamberlain appealed.

The Federal Circuit agreed that Chamberlain customers possessed an "inherent legal right to use" the software embedded in the GDOs.[74] Furthermore, addressing an issue of first impression the court of appeals held that for DMCA to apply, a plaintiff must establish that the circumvention of that TPM bears some "reasonable relationship to the protection that the Copyright Act otherwise affords."[75] Since consumers were entitled to access the GDO software, Chamberlain was unable to prove the critical nexus between the access facilitated by Skylink's device and the protection of a legitimate copyright interest.[76] In the same line of thought the Federal Circuit held in Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc., that "to the extend that rights under copyright law are not at risk, the DMCA does not create a new source of liability ".[77]

### *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc*

Storage Technology manufactured automated tape cartridge libraries capable of storing large quantities of computer data and it restricted access to the maintenance code using a password protection scheme. As defendant, Custom Hardware Engineering, was forced to "crack" or bypass this password in order to repair data libraries, Storage Technologies sued invoking Section 1201(a) (1) of the DMCA. Although the district court issued preliminary injunction, the Federal Circuit mandated. The court found it unlikely that Plaintiff would be able to prove that the circumvention password "either infringes or facilitates infringing a right protected by the Copyright Act'.[78]

Despite the fact that both Chamberlain and Storage should be praised for resisting the expansive interpretation of the DMCA embodied in Reimerdes, the two decisions didn't clarify the circumstances under which the nexus requirement

with copyright infringement will exist. This uncertainty may affect the application of the nexus requirement in cases concerning "entertainment" or "informational" goods, when it is not equally obvious that the copyright holders are trying to promote a profitable business model rather than protect their rights. Thus, there is a higher risk that courts will disregard the fact that copyright holders misuse TPMs to hamper competition in markets of more "artistic" copyright works.

### *Davidson & Assocs. v. Internet Gateway*

Davidson & Assocs. v. Internet Gateway [79], decided only one year after the Lexmark and Chamberlain decisions were issued, draws away from their line of thought and takes a step back towards Reimerdes.

Blizzard, the owner of copyrights in computer game software and online gaming service software, offered an online matchmaking service, Battle.net that allowed players to compete over the internet. Battle.net relied on a secret handshake with Blizzard games to validate unique CD keys. Defendants (bunted team) reverse engineered the protocols used by Blizzard games to communicate with Battle.net and developed alternative service software that interoperated with Blizzard games. However, since bnetd lacked access to Blizzard's database of CD keys, it was unable to ensure that all players used legitimate copies of Blizzard games. Blizzard sued the bnetd for breach of contract, circumvention of copyright protection system, and trafficking in circumvention technology. In response, Bnetd raised the interoperability exception as one of its defences, arguing that any circumvention of Blizzard's access controls occurred to enable reverse engineering meant to render the bnetd server software interoperable with Blizzard games and any tools it distributed that facilitated circumvention were intended to enable interoperability.[80]

The district court rejected bnetd's Section 1201(f) defence arguing that, first, bnetd lacked permission to circumvent[81], secondly, the sole purpose of bnetd's circumvention was to "avoid the anticircumvention restrictions of the game and to avoid the restricted access to Battle.net"[82] and third because bnetd server was not an independently created computer program, since it was intended as a functional alternative to the Battle.net service, one that was indistinguishable from Battle.net from the standpoint of the users.[83]

The district court's analysis was flawed, resulting into practically nullifying the interoperability exception, even for defendants that fall squarely within the protections for reverse engineering and interoperability. Firstly, under the court's holding that bnetd could benefit from the interoperability exception only if it had permission to circumvent, Section 1201(f) becomes redundant, and as if bnetd had permission an affirmative defence would be unnecessary. Besides, by holding

that the sole purpose of the bnetd's circumvention was to avoid the anticircumvention restrictions, the court falls into a dangerous tautology; the circumventor's goal is always going to be to circumvent. Finally, the fact that bnetd server was intended as a functional alternative to the Battle.net service, that was indistinguishable from Battle.net, simply means that bnetd was successful in its attempt to enable interoperability, not that the bnetd server was not an independently created computer, as the court held.[84]

On appeal, the Eight Circuit, affirmed the district court's decision and held that bnetd's circumvention constituted infringement because unauthorized games of Blizzard games can be played on the server. The court erred in its holding, as the fact that some users connected to the bnetd server using unauthorized copies of Blizzard games does not prove that bnetd infringed Blizzard's rights under Section 106.

## The day after Lexmark, Chamberlain, Storage and Davidson

Lexmark, Chamberlain and Storage were all motivated by common concerns; the impetus behind them was an effort to restore competition in the market and allow interoperability. The courts realized that the companies were not interested into protecting their code from unauthorized access or copying, but were rather trying to promote a profitable business model and take advantage of the anticircumvention regulation to increase their market share.[85]

The same concerns though could be true in cases of manufacturers and vendors of products from the entertainment industry. Courts, however, have failed to apply a similar approach that addresses the interests of competitors and consumers in cases involving the use of TPMs to protect "informational" or "entertaining" works. Davidson indicates that courts may issue their decisions focusing on an evaluation of the risk of piracy disregarding the potential of distorting competition and follow an expansive or restrained application of the DMCA's liability provisions accordingly. If this ascertainment is true, we should hold our reservations as to the extend that the holding of the Lexmark, the Chamberlain and Storage holdings apply outside of the domain of tangible articles of commerce.

The approach that courts seem to follow, though, protects the interests of competitors and consumers in rather mundane commodities but fails to do the same for cultural artefacts.[86] The social harms generated by anticompetitive conduct in markets for informational and artistic goods are much higher. The traditional goal of Intellectual Property doctrine has been to provide incentives for the creation of as many and as diversified creative works as possible. Raising barriers to entry in markets of copyright works risks the quality and quantity of the produced works. Having a limited number of dominant firms controlling the production of creative works hinders the development of our culture and our civilization.

Anticircumvention regulation steadily leads to concentration in the creative markets, a goal that directly opposes the "progress of sciences and useful arts".

## The application of competition law and the misuse of anticircumvention legislation

Anticompetitive conduct issues are resolved as a rule by competition law in both sides of the Atlantic. As intellectual property rights, though, constitute limited monopolies, safeguards of healthy competition in the market are embedded within the intellectual property doctrine. Still, competition law authorities have intervened in the past in various occasions when intellectual property right holders have misused their monopoly power in expense of the market, especially in the EU.[87] As the misuse of anticircumvention legislation by the right holders harms competition in the adjacent markets at a cost to innovation and consumer welfare, it would be interesting to examine whether competition law could limit the control that TPMs yield over interoperable technologies. After all, competition law remedies and particularly the mandatory disclosure of technical information and the obligation to deal could facilitate interoperability.

In favour of relying on competition law to enable interoperability is the fact that courts and competition law authorities are less likely to be influenced by the lobbying efforts of the entertainment and software industry and thus may be more likely to strike the right balance between creative incentives and the creation of a robust public domain.[88] In addition, it has been argued that competition law allows for forward-looking remedies that may guard against technological efforts to disrupt healthy competition in the market.[89] Of course, it should be noted that some scholars and courts have argued that courts are ill suited to assume the day to day control of the enforcement of the remedy.[90] However, the most significant practical disadvantage of relying on competition law to "correct" the implications of anticircumvention regulation is timing. In innovation markets, the ability for the authorities to interfere immediately and restore healthy competition is fundamental, because of the network effects that are created in the market. If consumer lock-in has already occurred, it is very hard to undo the consequences of an anticompetitive practice.[91] Amending anticircumvention legislation itself, and thus fixing the source of the problem, so that the Intellectual Property regime would afford developers and vendors of interoperable products immediate self-help is far preferable to providing them with competition law remedies some years subsequently.[92]

More importantly, because of the way that competition law doctrine and jurisprudence is formulated on both sides of the Atlantic, competition law appears unlikely to disturb the enforcement of the broad grants provided by anticircum-

vention regulation, for two basic reasons. First, both Section 2 of the Sherman Act and Article 102 TFEU impose a minimum threshold of market power in order to hold a conduct as anticompetitive. Secondly, competition law gives substantial deference to the lawful exercise of legitimately acquired intellectual property rights, especially in the United States.

The decision to exclude from the operation of the law competitors who do not have a dominant position and monopoly power in the relevant markets does not mean that the conduct of those competitors does not hinder competition. The condition of dominant position and monopoly power exists to ensure that competition law will not lead to over-deterrence of firms from engaging in the competitive process. Market power is solely an indication of the likelihood of anticompetitive effects.[93] The market power condition is important. Otherwise, all firms would risk violating competition law. Such a risk stifles desirable business activity because anti-competitive effect is not always easy to discern ex ante. For this reason competition law chooses to examine the conduct of firms only when they are most likely to engage in anticompetitive practices.[94] Therefore, to avoid over-deterrence, lawmakers are willing to permit some anticompetitive behaviors. However, as argued above, timing is crucial in innovation markets. This means that when a competitor unlawfully gains a dominant position, it may be too late for the authorities to intervene.

Thus, competition law rules are too rigid to apply efficiently in cases of anticompetitive misuse of the anticircumvention provisions, pointing to the conclusion that these anticompetitive behaviours should be dealt with inside the field of anticircumvention law.

## The need for amendment of the anticircumvention provisions

### *European Union*

Since judicial interpretation of the European anticircumvention legislation does not have the flexibility to balance the risks of tolerating piracy on the one hand with fragmenting the market on the other and since competition law is not capable of restoring this balance an amendment of the existing legislation at an EU level seems indispensable.

Substantively, it is suggested that the Community legislator should limit the protection of TPMs to copy controls and add an explicit requirement that a circumventor of a TPM can infringe the anticircumvention regulation only if her act is a violation of a valid copyright or neighbouring right. Such a modulation would limit the effects of anticircumvention regulation to combating piracy and would not provide to copyright holders an additional right to control all the uses of their

works in the digital environment by taking away this right from the public. This proposed amendment is congruent with the traditional theory of Intellectual Property law, according to which, copyright constitutes a limited exception to the right of the public to have access to creative works.

Furthermore, the requirement of the Software Directive that for a device to be held as violating the anticircumvention regulation sole purpose should be to circumvent an effective TPM should be extended to the Information Society Directive; alternatively the ECJ should interpret the "limited commercially significant purpose or use other than to circumvent" requirement in way that legalizes the circumvention of TPMs to achieve lawful purposes that enhance the uses of the copyright works and raise barriers to entry. Under such a legal regime competitors will be able to break the technical barriers to entry into new markets that first comers or dominant firms in adjacent markets raise.

Turning now to the exceptions to copyrights, the following major changes appear as essential. Firstly, all the exceptions to rights on copyright works that a Member States provides should automatically apply with respect to TPMs; secondly, the exceptions should constitute exceptions to the liability of circumvention of the TPMs.[95]

Of course if the violation of anticircumvention legislation becomes dependant upon a violation of copyright law by the circumventor, the latter modification would be redundant; to elaborate, despite the fact that access or copying the copyright work would be legally protected by the TPM, the beneficiary of an exception will be entitled to access or copy it and thus she will not be violating copyright law or neighbouring rights. Consequently, as the beneficiary will not be violating copyright law, she will not be violating the anticircumvention provisions either. If the anticircumvention legislation, though, does not have an auxiliary character to copyright law, and it provides a further right to the copyright holder to control the uses of copyright work, as it does today, it is crucial that the legislation at least ensures that the beneficiaries of exceptions to copyright are not forfeited by their rights.

Moreover, the exceptions in the Information Society Directive also do not include reverse engineering, [96] although such an exception exists in the Software Directive, which provides a limited safe harbour for those trying to achieve software interoperability.[97] From the Recitals of the Software directive and from its legislative history we can infer that the Community legislator wanted to encourage connecting all components of a computer system, including those of different manufacturers, so that they can work together.[98] The cooperation between manufacturers is a noble objective also in the fields of traditional copyright goods. Through cooperation of authors of artistic works the output of such works will

increase creating a richer and fuller culture for European Citizens. The exclusive focus of this exception on computer programs must be abandoned in favour of an exception that applies in all classes of copyright works, recognizing the role that data plays in enabling system-level interoperability.[99]

Finally, it is crucial for European Union not to differentiate the treatment of tangible articles of commerce and to cultural artefacts. All the above substantive amendments, thus explicitly requiring "violation of a valid copyright or neighbouring right" for the affirmation of infringement of anticircumvention regulation, introducing the "sole purpose to circumvent an effective TPM" requirement for the affirmation of infringement of anticircumvention regulation and introducing an "interoperability exception" should apply equally to consumer electronics products and informational and entertaining goods.

### *United States*

After Lexmark, Chamberlain and Storage Technologies courts have tried to narrow the scope of the DMCA by demanding a nexus between a copyright violation and a DMCA infringement, and expanding the "effective restriction of access to copyright works" requirement for the protection of TPMs. However, courts may abandon this approach in the case of manufacturers of goods that fall under the traditional definition of copyright works. [100]

Thus, the legislator is the appropriate organ to balance the need for protection of copyright works on the one hand with the need to safeguard healthy competition in the "creative" markets. The scale should turn towards healthy competition, as innovation can be achieved only within a free market. Furthermore, a dispersed market of creative works advances diversification and variety in the arts and culture and promotes the development of civilization. Thus, the legislator should amend the DMCA to ensure that it does not lead to the creation of further monopolies, which the legislator initially did not aim to protect and that are not subject to the restraints imposed on Intellectual Property rights. After all, overincentivizing authors of 'creative' works can have reverse effects than the ones expected, since when the level of protection is too high, creation and innovation are impeded rather than promoted.

In order to achieve the right balance between protecting competition in the secondary markets and promoting the interests of copyright holders the legislator should amend the DMCA in the following ways:

Firstly, a clause should be added that would ban the differential treatment of tangible articles of commerce and cultural artefacts and that shall instruct courts to apply all the provisions of the DMCA equally to both kinds of works.

Secondly, the legislator should explicitly condition the three causes of action of Section 1201 under the infringement of a valid copyright. The plaintiff should bare the burden of proving that her copyrights are infringed.

Thirdly, Section 1201(f) should be amended to explicitly create a safe harbour for circumventing TPMs protecting all kinds of copyright works and to protect data operability as well.

The most important consequence of the legislative intervention is that it will create a safety regarding the actions that a competitor is allowed to undertake, thus promoting competition and innovation. Furthermore, the altered legislative environment will discourage copyright holders from misusing TPMs in the detriment of their competitors and of consumer welfare. The power that the legislator has to form behaviors can not be compared with the effects of judicial intervention. This power makes an amendment of the law urgent as the disparity of decisions and the broad holdings have created an uncertainty that encourages anticompetitive conducts by copyright holders.

## Concluding remarks

Academics have been warning for a long time that intellectual property laws are being rewritten in ways that neglect values embedded in neighbouring legal fields, such as contract, competition and free speech law. [101] Anticircumvention regulation constitutes an example of such move away from the traditional Intellectual Property law. It strengthens the rights of copyright holders at the expense of healthy competition and consumer welfare. As a result of anticircumvention regulation copyright owners enjoy three cumulative layers of protection: the legal protection of copyright law, the technical protection of their works achieved by TPMs and the legal protection against the circumvention of the TPMs.

Vendors and manufacturers of consumer primary products, who hold a dominant position in the primary product market, can use anticircumvention regulation in order to reinforce their dominant market position in the aftermarket by preventing interoperability of products on alternative systems. Unfortunately (The) judicial interpretation of the EU and US anticircumvention legislation does not have the flexibility to balance the risks of tolerating piracy on the one hand with fragmenting the market on the other and competition law is not capable of restoring this balance; Therefore, the existing legislation at an EU level as well as in the US needs to be amended. On the one hand, the infringement of the anticircumvention norms should be explicitly conditioned to the infringement of a valid copyright and on the other there should be no differentiation in the treatment of tangible articles of commerce and cultural artifacts and courts should be instructed to apply all exceptions equally to both categories of works.

It is important to keep in mind that, just like any technology, TPMs are in themselves neutral; but, when used, are capable of both producing both "good" and "bad". However anticircumvention regulation on both sides of the Atlantic allows, if it does not encourage, uses of TPMs that reduce consumer welfare and harm competition and thus it needs to be amended.

## Endnotes

* PhD Candidate Cantab, LL.M. Harvard. This paper is a provisional draft and should not be cited without the permission of the author. The author may be contacted at pv250@cam.ac.uk.

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 legale des systemes 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. DeWerra, '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 Congress on Adjuncts and Alternatives to Copyright. On TPM and fair use see Grodzinsky F. Bottis M., Privateuse as fair use - is it fair? ACM SIGCAS Computers and Society , Volume 37, issue 2, 2007, pp. 11-24.
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.
3. Indicatively see C. Clark, 'The Answer to the Machine is in the Machine', in P. B. Hugenholtz (ed.) The Future of Copyright in a Digital Environment (1996), p.139; A. Dixon &L. Self, 'Copyright Protection for the Information Superhighway' 11 EIPR 465(1994); J. C. Ginsburg, 'Putting Cars on the "Information Superhighway": Authors, Exploiters and Copyright Cyberspace', 95 Columbia Law Review 1466 (1995); B. Lehman, 'Intellectual Property and the National and Global Information Infrastructures' in P. B. Hugenholtz (ed.) The Future of Copyright in a Digital Environment (1996), 103.
4. Indicatively see Y. Benkler, 'Free As the Air To Common Use: First Amendment Constraints on the Enclosure of the Public Domain',74 N.Y.U. Law Review 354 (1999); J. E. Cohen, 'Copyright and the Jurisprudence of Self-Help', 13 Berkeley Tech. L. J. 1089 (1998); Ibid., 'A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace', 28 Connecticut Law Review 981 (1996); Ibid., 'Some Reflections on Copyright Management Systems and Laws Designed to Protect them', 12 Berkeley Tech. L. J. 161 (1997); S. Dusollier, 'Tipping the Scale in Favour of the Right Holders: The European anticircumvention Provisions', in E. Becker, W. Buhse, D. Günnewig, N. Rump (eds.) Digital Rights Management. Technological, Economic, Legal and Political Aspects (2003) 462; K.J. Koelman, 'A Hard Nut to Crack: the Protection of Technological Measures' 22(6) EIPR 272 (2000), at 275; J. Litman, Digital Copyright (2006); Ibid., 'Sharing and Stealing' 27 Hastings Communications and Entertainment L. J. 1 (2004); N. W. Netanel, 'Locating Copyright Within the First Amendment Skein', 54 Stanford Law Review 1 (2001); P. Samuelson, 'Intellectual Property and the Digital Economy: Why the anticircumventionRegulations Need to be Revised', 14 Berkeley Tech. L. J. 519 (1999); T. C. Vinje, 'A Brave New World of Technical Protection Systems: Will There Still

be room for copyright', 18 EIPR 431 (1996); G. Westkamp, 'Transient Copying And Public Communications: The Creeping Evolution Of Use And Access Rights In European Copyright Law' 36 George Washington International Law Review 1057 (2004), at 1078.

5. Many printer cartridges come with chips that authenticate them to the printer, a practice that started in 1996 with the Xerox N24. In a typical system, if the printer senses a third-party cartridge, or a relled cartridge, it may silently downgrade from 1200 dpi to 300 dpi, or even refuse to work at all. An even more recent development is the use of expiry dates. Cartridges for the HP BusinessJet 2200C expire after being in the printer for 30 months, or 4.5 years after manufacture. See Ross Anderson, Cryptography and Competition Policy – Issues with "Trusted Computing", 1, available at: http://www.cl.cam.ac.uk/~rja14/Papers/tcpa.pdf.
6. Among them, Apple's use of the "chain of Trust" in its popular iPhone device that prevents subscribers from installing applications from third parties is worth mentioning.
7. The term effective is circularly defined as "an access control or protection process" which "achieves the protection objective", Article 6(3) of the Information Society Directive.
8. Article 6(1) of the Information Society Directive provides that "Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.", whereas Article 6(2) of the Directive provides that "Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

   (a) are promoted, advertised or marketed for the purpose of circumvention of, or

   (b) have only a limited commercially significant purpose or use other than to circumvent, or

   (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of any effective technological measures."
9. A linklist to international and national legislation on technological protection measures with focus on the relevant laws of EU member states has been made available at <http://cyber.law.harvard.edu/media/eucd> by the Berkman Center's Digital Media Project team. As regards the failure of the Information Society Directive to efficiently harmonize European law, which after all was the impetus behind the directive, especially in regard to the exceptions of TPMs legal protection see B. W. Elser, Technological Self-Help: Its Status under European Law and Implications for U.K. Law, BILETA, 17th BILETA Annual Conference, April 5th -6th, 2002, Free University of Amsterdam, p. 12 available at: http://www.bileta.ac.uk/02papers/esler.html in Peter Prescott et al., The modern law of copyright, Ch. 20 (3rd Ed. 2000), at 12.
10. On the definition of TPMs in Article 6(3) of the Information Society Directive see above note.
11. Urs Gasser, Michael Girsberger, Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States. A Genie Stuck in the Bottle?, Berkman Publication No. 2004-10, available at: http://cyber.law.harvard.edu/publications.
12. Article 6(4) and Articles 5(2)(a), 5(2)(c), 5(2)(d), 5(2)(e), 5(3)(a), 5(3)(b) and 5(3)(e) of the Information Society Directive. For a critical comment on Art. 6(4) see Dussolier, Exceptions and technological measures in the European Copyright Directive of 2001 – an empty promise, 34 I.I.C.62 et.seq (2003).

13. Information Society Directive, Recitals 51-53.
14. Nora 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 E.I.P.R. 11, 496, 499 (2003).
15. Information Society Directive Article 6(4) and Recital 50. The enactment of exceptions to TPMs conditioned upon "the absence of voluntary measures taken by right holders" has been criticized as "making law making power contingent upon the acquiescence of corporate and private interests" and that "rightholders[…] may use Article 6(4) as a sword of Damocles over the heads of national legislatures, threatening them with challenges to their authority to govern the scope of copyright and its related rights. " B. W. Elser, supra note 11 at 12.
16. Esler, supra note 11, at 12, arguing that "Without Article 6(4), it would be clear – pursuant to Article's 6(3) definition of "technological measures" – that any exceptions adopted would apply equally to TPM circumvention, i.e. circumvention in furtherance of an exception would not fall afoul of the law. By calling out eight specific exceptions which must be applied (at least "in the absence of voluntary measures taken by right holders, the clear implication is that other exceptions do not have to apply with respect to TPMs.)". However, we should note that Elser believes that "it would make more sense to apply all exceptions equally to TPMs" and suggests that the UK should do so.
17. Cf Article 5 with Article 6(4).
18. Access controls are TMPs intended to prevent unauthorized access to copyright works, or according to the wording of 17 U.S.C. 1201(a)(3)(B) "in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work".
19. Copy controls are TPMs intended to prevent infringement of the exclusive right afforded by copyright, or according to the wording of 17 U.S.C. 1201(b)(2)(B) "in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title".
20. Section 1201(a)(3)(A) defines anticircumvention as descrambling a scrambled work, decrypting an encrypted work, or otherwise avoiding, bypassing, removing, deactivating, or impairing a technological measure, without the authority of the copyright owner.
21. The DMCA provides both civil remedies and criminal sanctions for the violation of the aforementioned provisions. Violators will be sued in front of the federal court [17 U.S.C. Section 1203(a)] and the complaining party may elect to receive either the sum of the actual damages it suffered and the additional profits earned by the violator, or statutory damages [Id. para 1203(c)]. In addition to that, violators that are prosecuted criminally may face sanctions up to a USD 500,000 fine and five-year imprisonment for any para 1201 and the penalty will be doubled for a second violation [Id. para. 1203(c) and 1203(a)].
22. The exemptions from anticircumvention provisions include conducting encryption research (17 U.S.C. Section 1201(g)), assessing product interoperability (Section 1201(f)) and testing computer security systems (Section 1201(j)). Exemptions under narrow circumstances are also provided for nonprofit libraries, archives and educational institutions "solely to make a good faith determination of whether to acquire a copy of that work" (Section 1201(d)).

23. For the congressional recognition of the permissibility of reverse engineering and the value of interoperability, see S. Rep. 105-190, at 32 (1998).
24. Section 1201(f)(1).
25. Section 1201(f)(3).
26. See Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, at 218 (S.D.N.Y. 2000); the Court rejected defendant's 1201(f) defence holding that the interoperability exception applies only to the circumvention of TPMs that restrict access to computer programs, not copyright works generally. For a discussion of the shortcomings of Section 1201(f) and why the statute needs to protect all interoperable technologies. Furthermore, the interoperability restriction fails to accommodate reverse engineering for other legitimate purposes. For example 1201(f) is not applicable in the cases of reverse engineers who extract uncopyrightable processes and principles to create non-interoperable products, or in the case of researchers who investigate the operation of TPMs. As regards the latter, although the encryption research and the security testing exceptions offer researchers some protection, the conditions set by Sections 1201(f) and (g) are very strict. For a discussion of the impact of Section 1201(g) on encryption research, see Joseph P. Liu, The DMCA and the Regulation of Scientific Research, 18 Berkeley Tech. L. J. 501 (2003). For a discussion of the benefits to the public that TPM research can offer outside of the encryption context see K. Mulligan & Aaron K. Perzanowski, The Magnificence of a Disaster: Reconstructing the Sony BMG Rootkit Incident, 22 Berkeley Tech. L. J. 1157 (2007) and Comment of J. Alex Halderman, In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Docket No. RM 2008-8 http://www.copyright.gov/1201/2008/comments /halderman-reid.pdf.
27. However, a case is pending in front of the ECJ.
28. The European Court of Justice has issued decisions against Portugal (Case C-61/05), Spain (Case C-31/04), France (Case C-59/04), United Kingdom (Case C-88/04), Finland (Case C-56/04), Sweden (Case C-91/04) and Belgium (Case C-143/04) because they failed to adopt the laws, regulations and administrative provisions necessary to comply with the Information Society Directive.
29. For example the Court of Fist Instance took into account emails sent to the defendant that showed that the principal purpose for which the mod chip was sought was to enable the playing of illegally copied games.
30. The Sezione per il riesame, in its interlocutory decision of December 31, 2003 held that the main function of the mod chip was to overcome "monopolistic obstacles and to make a better use of the console". The Court of Appeals held that the use of the chip allowed the use of the console to its full potential.
31. For the financial data regarding the video gaming industry see: Robert W. Crandall & J. Gregory Sidak, video games: serious business for america's economy § 2, at 7 (2006), available at: http://papers.ssm.com/sol3/papers.cfm?_abstract_id=969728.For a discussion of gaming culture and social norms and their evolution as well as the methods that the gaming industry has employed to alter these norms see: Corinne L. Miller, The Video Game Industry and Video Game Culture Dichotomy: Reconciling Gaming Culture Norms With the anticircumvention Measures of the DMCA, 452 Texas Intellectual Property L. J. 16.
32. Anderson, supra note 7.

33. Sony has succeeded in preventing the playing of unauthorized video games by enforcing and protecting the measures it incorporates into the consoles in the United Kingdom. See Kabushiki Kaisha Sony Computer Entertainment v. Ball [2005] FRS 9. In the US, see Sony *Computer Entertainment America Inc v. Gamemaster,* 87 F.Supp. 2d 976 (ND Cal 1999). Sony failed in Australia: see *Stevens v. Kabushiki Kaisha Sony Computer Entertainment* [2005] HCA 58. For the US case, see below under Part IV section 2.
34. The court also expressed dissatisfaction with Sony's practice of dividing the world into three regions and providing its games with codes depending on the region in which they were purchased. The result of the region-coding system was that games could only play in consoles purchased in the same region as the game. Sony changed this practice in November 2006, when it launched PlayStation 3.
35. Legge 22 April 1941, n 633, amended by Decr. Leg. No 68, 9 April 2003 (Henceforth Lda).
36. Article 102 quarter of the Lda expressly permits the holder's of author's rights and related rights to apply effective TPMs to their works.
37. Decision of the Sezione per il riesame of the Tribunale di Bolzano, 31 December 2003, ECDR 18, 2006, online available at: http://www.ictlex.net/?p.
38. In this regard, the court provided a "real world metaphor". It suggested that Fiat could not sell a car with the condition that it not be driven by foreigners or on country roads.
39. Tribunale di Bolzano - Sentenza del 28 gennaio 2005 (Playstation modificate - 2), available at: http://www.interlex.it/testi/giurisprudenza/bz050128.htm.
40. The court held that the TPMs employed by Sony should be protected under the act, "because they operated to prevent acts not authorized by the right holder".
41. According to the court's ruling the use of imported games on consoles was considered illegitimate. This was because Article 17 prohibited importation from outside the European Union. However, this argument is ill-founded, because Art 17 prohibits only importation for the purposes of distribution, therefore not preventing individual imports. The argument that mod chips permitted the reading of back-up copies was also rejected, because the right to make back up copies applies only to software. According to Article 71sexies, the right to make a copy of other copyright works must respect any TPMs applied to the work. Evidence of emails sent to the accused showed that the principal purpose for which a mod chip was sought was to enable playing of illegally copied games.
42. Tribunale di Bolzano - Sentenza del 20 dicembre 2005 (Playstation modificate - 3), available at: http://www.interlex.it/testi/giurisprudenza/bz051220.htm.
43. Cassazione, Sezione III Penale, Sentenza 25 maggio 2007 (dep. 3 settembre 2007), n. 33768 (35598/2006), available at http://www.civile.it/newS/visual.php?num=45307.
44. Tribunale Civile di Milano, Sezione proprietà industriale e intellettuale, Sentenza 5 Marzo 2009. An overview of the decision is available at http://www.dirittodautore.it/page.asp?mode=News&IDNews=4675&idcan=2.
45. Dan L. Bruk. Legal and Technical Standards in Digital Rights Management Technology, 74 FORDHAM L. REV. 537, 570 (2005), arguing that "the anticircumvention provisions may therefore play the role that patents sometimes play in suppressing device interoperation".

46. Steven P. Calandrillo and Ewa M. Davison, The Dangers of the Digital Millennium Copyright Act: Much Ado About Nothing?, WILLIAM & MARY LAW REVIEW, Vol. 50, 349, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262042 .
47. 87 F. Supp. 2d. 976 (N.D. Cal. 1999).
48. See also Calandrillo & Davison, supra note 48, 18.
49. Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, (S.D.N.Y. 2000), aff'd sub nom. Universal City Studios, Inc. v. Coley, 273 F.3d 429 (2d Cir.2001) affirming the constitutionality of the DMCA on challenge by defendant Corley form the district court. The court asserted that the DMCA "fundamentally altered the landscape" of copyright.
50. The importance of Reimerdes is also illustrated by the fact that another maker of DVD copying software, similar to DeCss, filed a complaint for declaratory relief against movie studies in the Federal District Court of the Northern District of California, the court followed verbatim the court's opinion in Reimerdes. To elaborate, 321 sought a declaration that its products did not violate Section 1201 of the DMCA and also challenged the constitutional validity of the statute. The court held that 321's copying software was primarily designed to circumvent CSS-protected DVDs, a violation of the anticircumvention rule. See 321, 307 F. Supp. 2d 1085 (N.D.Cal. 2004) *Studios v. Metro Goldwyn Mayer Studios, Inc,*.

    Note, that in 321 Studios the Federal District Court of the Northern District of California followed Southern District of New York opinion in Reimerdes and held.
51. Id. at 316-317. As regards the application of the Sony test for determining liability applied, the court held that "to the extend of any inconsistency between Sony and the new statute" Sony is overruled.
52. Id. at 314; the court stated "At trial defendants repeated, as if were a mantra, the refrain that plaintiffs [...] have no direct evidence of a specific occasion on which any person decrypted a copyrighted motion picture with DeCSS[...]. But this is unpersuasive."
53. Id. at 218.
54. Id.
55. *Davidson & Assocs. v. Internet Gateway*, 334 F. Supp. 2d 1164 (E.M. Mo. 2004), aff'd' sub nom, 422 F. 3d 630 (8th Cir. 2005).
56. Note that no defendant has yet succeeded on a Section 1201(f) defence. See Perzanowski, supra note 28, 22.
57. Css, also known as "Content Scramble System" is a TPM encoded on DVDs by the Movie Industries to control access to the movies. DeCss was the software used to overcome Css. Id. at 308-309.
58. See the language of Section 1201(f)(1).
59. The court rejected Defendants argument that the sole purpose of the DeCSS software used to overcome the TPMs was to enable interoperability with Linux-based DVD player software, arguing that as DeScc also enabled interoperability under Windows, where there was no compatibility concern. Reimerdes, 111F.Supp.2d. at 218.
60. Section 1203(f)(3) verbatim provides "The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if [...]" (emphasis added).

61. See Perzanowski, supra note 28, at 22, footnote No. 92.
62. Jerome H. Reichman, Graene Dinwoodie, Pamela Samuelson, A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works, 22 Berkeley Tech. L. J. 981, 1005-1006, 1024 (2007).
63. *Lexmark Int'l, Inc. v. Static Control Components, Inc.,* 387 F.3d 522, 530 (6th Cir. 2004).
64. Each time a printer was turned on, the printer and cartridge initiated a authentication sequence whereby each would calculate a code using an encryption algorithm. Static Control Components. Id at 350.
65. Id. 530-531.
66. *Lexmark Int'l, Inc. v. Static Control Components, Inc.,* 233 F. Supp. 2d 943, 974(E.D. Ky. 2003).
67. 381 F.3d. at 546-47.
68. Id.
69. See S. Callandrio & E. Davison, supra, 39-42.
70. After all, if Lexmark had restricted access to its authentication sequence more fully, perhaps by encrypting the product code, its DMCA claim could have moved forward. See Perzanowski, supra note 28, 24. But See also Judge Merritt's concurrence, warning that future litigants could not escape the court's hostility to similar claims through minor variations on the Lexmark facts, 387 F.3d at 551-52 (Merritt, J., concurring).
71. *Chamberlain Group, Inc, v. Skylink Techs,* 292 F. Supp. 2d 1040 (N.D. III.2003).
72. *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc,* 421 F.3d 1307, 1318 (Fed. Cir. 2005). Storage Technology manufactured automated tape cartridge libraries capable of storing large quantities of computer data and it restricted access to the maintenance code using a password protection scheme. Defendant, Custom Hardware Engineering, was forced to "crack" or bypass this password in order to repair data libraries. Storage Technologies sued invoking Section 1201(a)(1) of the DMCA and although the district court issued a preliminary injunction, the Federal Circuit found otherwise.
73. See also Perzanowski, supra note 28, 25.
74. 381 F.3d at 1202.
75. Id.
76. Id. at 1203.
77. *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc,* 421 F.3d 1307, 1318 (Fed. Cir. 2005). Storage Technology manufactured automated tape cartridge libraries capable of storing large quantities of computer data and it restricted access to the maintance code using a password protection scheme. Defendant, Custom Hardware Engineering, was forced to "crack" or bypass this password in order to repair data libraries. Storage Technologies sued invoking Section 1201(a)(1) of the DMCA and although the district court issued preliminary injunction, the Federal Circuit found it likely.
78. Id. at 318.
79. Davidson & Assocs. V. Internet Gateway, 334 F. Supp. 2d 1164 (E.D. Mo. 2004), aff'd sub nom, 422 F.3d 630 (8th Cir. 2005). For an elaborate discussion of the Davidson case

see: Paul J. Neufeld, Circumventing the Competition: he Reverse Engineering Exemption in DMCA § 120, 26 The Review Litigation, 525(2007); Perzanowski, supra note 28, 32.

80. 334 F. Supp. 2d at 1183.
81. Id. at 1185.
82. Id. at 1186.
83. Id. at 1185.
84. See also Perzanowski, supra note 28, 32.
85. See also ibid stating: "Both courts worried that by adding fragments of copyrighted code to consumer goods, manufacturers could "gain the right to restrict consumers' rights to use [their] product in conjunction with competing products (Chamberlain, 381 F.3d at 1201). Such power, in turn, could "create monopolies of manufactured goods" (Lexmark, 387 F.3d at 1201) that relied on the DMCA to provide "broad exceptions from all [ ]antitrust laws"(Chamberlain, 381 F.3d at 1201). "
86. Nina Elkin-Koren, Making Room for the Consumer under the DMCA, 22 Berkeley Tech. L. J. 1119, (2007).
87. See Joined cases C-241/91 P and C-242/91 P, *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission* (Magill), 1995 E.C.R. I-00743; Case T-65/98R, Van den Bergh Foods, 2003 E.C.R. II-4653; Case C-418/01, *IMS Health v NDC Health,* 2004 ECR I-5039, paragraph 49; T-201/04, *Microsoft v Commission,* 2007 E.C.R. II-3601, paragraphs 319, 330, 331, 332 and 33; See also *Microsoft III,* 253 F. 3d 34, 58(D.C. Circuit 2001).
88. Herbert J. Hovenkamp, Innovation and the Domain of Competition Policy, 103 A. LA. L. Rev. 16 (2008).
89. Perzanowski, supra note 28, 39.
90. Phillip Areeda, Essential Facilities: An Epihtet in Need of Limiting Principles, 58 Antitrust L. J. 841, 853 (1989) arguing that an antitrust remedy should not be available "when compulsory access requires courts to assume the day to day controls characteristic of a regulatory agency". *Verizon Comms. v. Law Offices of Curtis V. Trinko,* 540 US 398, 414 (2004).
91. The Microsoft case seems to be a perfect example of that. Although Microsoft lost in court in both sides of the Atlantic, the remedies imposed could not restore competition in the market. Microsoft Corp., T-201/04, 249 (CFI Sept. 17, 2007) requiring Microsoft to disclose protocol specifications that enabled interoperability between Windows and work group server operating systems; United States v. Microsoft, 97 F. Supp. 2d 59, 67 (D.D.C. 2000) requiring disclosure of APIs, Communication Interfaces, and Technical Information used to enable interoperability; United States v. Microsoft, 231 F. Supp. 2d 144. 186-195, approving settlement agreement containing provisions for mandatory disclosure of interoperability information; United States v. Microsoft, 2006 U.S. D.D.C. Sept. 7, 2007, Modified Final Judgment.
92. Phillip J. Weiser, The Internet, Innovation, and Intellectual Property Policy, 103 Colum. L. Rev. 534, 551-52 (2003) arguing that the speed of reverse engineering self-help renders it preferable to an antitrust conduct remedy.
93. Adrian Majumbar, Whither Dominance, 4 E.C.L.R. 161, 162 (2006).
94. Einer Elhauge & Damien Geraldin, Global Antitrust Law and Economics 256 (2007).

95. Note that if a requirement that a circumventor of a TPM can infringe the anticircumvention regulation only if his/her act is a violation of a valid copyright or neighbouring right is enacted, such a provision.

96. See also Recital 50 of the Information Society Directive: "Such a harmonised legal protection does not affect the specific provisions on protection provided for by Directive 91/250/EEC. [...] Articles 5 and 6 of that Directive exclusively determine exceptions to the exclusive rights applicable to computer programs."

97. Article 6 of the Software directive provides that 1. The authorization of the right holder shall not be required where reproduction of the code and translation of its form within the meaning of Article 4 (a) and (b) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

    (a) these acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorized to to so;

    (b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in subparagraph (a); and (c) these acts are confined to the parts of the original program which are necessary to achieve interoperability.

    2. The provisions of paragraph 1 shall not permit the information obtained through its application:

    (a) to be used for goals other than to achieve the interoperability of the independently created computer program;

    (b) to be given to others, except when necessary for the interoperability of the independently created computer program; or (c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

98. See Recitals of the Software Directive: "Whereas an objective of this exception is to make it possible to connect all components of a computer system, including those of different manufacturers, so that they can work together".

99. See Perzanowski, supra note 28 arguing that "TPMs can not be neatly divided between those that restrict the use of entertainment content and those that control the use of computer programs. Frequently, the same TPM serves both functions", therefore the unavailability of an interoperability exception as regards entertainment content "ignores the role of data in enabling interoperable relationships, hampering the exceptions ability to fully accommodate interoperability" with further reference to Urs Gasser & John Palfrey, Drm-Protected Music Interoperability and Einnovation 21(2007), http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/interop-drm-music 0.pdf.

100. From the enactment of the DMCA many proposals have been articulated that would allow permissible uses of copyright works that are currently restricted under Section 1201. Dan Burk has argued that anticircumvention law requires its own doctrine of misuse (Dan L. Burk, Anticircumvention Misuse, 50 UCLA L. REV. 1095 (2003) 88). Timothy Armstrong has suggested that courts should more readily draw on fair use principles to create a body of judge-made fair circumvention law (Timothy K. Armstrong, Fair Circumvention, Brooklyn Law Review, Vol. 74, No. 1, pp. 1-50, 2008; U of Cincinnati Public Law Research Paper No. 08-08. Available at SSRN: http://ssrn.com/abstract=1095876 ). Aaron Per-

zanowski suggested to broaden the DMCA's existing interoperability exception to create an environment more hospitable to interoperable technologies (A. Perzanowski, supra 26.) Jerome Reichman, Graeme Dinwoodie and Pamela Samuelson have proposed a reverse notice and take down regime under which rights holders would be obligated to remove TPM restrictions after user-notification of a desire to make lawful uses of TPM-protected works (Jerome H. Reichman et al., supra note 62, 119). Each of this proposals have substantial merit and would address the many unintended consequences of the DMCA, but none of this proposals specifically address the importance to safeguard competition in the artistic markets.

101. Indicatively see William W. Fisher III, Reconstructing the Fair Use Doctrine, 101 Harv. L. Rev. 1659 (1988); Margaret Jane Radin, A Comment on Infrormation Propertization and Its Legal Milieu, 54 Clev St. L. Rev. 23 (2006); Neil Weinstocl Netanel, Copyright and a Democratic Civil Society, 106 Yale L. J. 283 (1996). On fair use in the EU and US, see Grodzinsky F. & Bottis M., Private use as fair use, is it fair? ACM SIGCAS Computers and Society vol. 37, issue 2, 2007, pp. 11-24.

# Constraints for introducing a "hadopi" law: the example of Greece

**Georgios N. Yannopoulos**

## HADOPI laws in france

### *HADOPI-1*

Even non-US cognoscenti are aware that in baseball games the batter has three chances to hit the ball thrown by the pitcher; if not, the batter goes out of the game and is replaced by another player ("*three strikes and he's out*"). The relevant French bill, inspired by this rule and following the guidelines of president Sarkozy, has been presented for the first time in November 2007. It has been based upon a report of a special task force headed by the managing director of French department stores FNAC Denis Olivenne. FNAC is one of the biggest proprietors of IP rights in France. The report has been endorsed by 40 media and entertainment representatives and has been presented as an agreement in order to foster the bill ("*Olivenne Agreement*" see http://www.edri.org and http://www.armt.fr).

The basic idea was simple: an independent administrative authority (*Haute Autorité pour la Diffusion des oeuvres et La Protection des Droits sur Internet* and hence the acronym HADOPI) is being established as the watchdog of intellectual property rights over the Internet. Ideally, HADOPI should handle complaints originating from the creators/proprietors of IP rights. In the next step the Authority should make research in order to verify the complaints upon information provided by internet Service Providers.

"Suspects" for illegal downloading would receive two warnings: In the first warning the "suspect" would be urged to thoroughly check whether third parties are using his/her internet connection (for example by tampering wireless networks). The user would be held exclusively liable to take necessary steps in order to reinforce the security of his/her network and could not claim later "wireless" taping as an excuse. If the "suspect" ignores the first warning and a second infringement takes place, within the six months following the first warning, the a second warning is being sent. If another infringement takes place within a year following second warning, then the Authority is entitled to decide the interruption of internet service access for a period varying between one month and one year; still the user-"suspect" must pay the fee to the Internet Service Provider, even for the periods of interrupted service. Furthermore, a system similar to the black list of

bankers, is established in order to avoid the change of provider for the period of interruption.

## *The history of HADOPI bills in France*

The draft bill had been presented to the French Senate (Sénat - http://www.senat.fr/-dossierleg/pjl07-405.html) by the government on 18th June 2008 under the name: Law to support the diffusion and the protection of the creation on the Internet (Loi favorisant la diffusion et la protection de la création sur Internet). On 23rd October 2008 the bill has been characterised as "urgent", having as a result only one reading per legislative chamber (National Assembly and Senate). On 30th October 2008 the bill has been voted at a first reading by the French Senate following two days of discussions.

The bill was then presented to the French National Assembly (*Assemblée Nationale*) on 11th March 2009 and an amended version has been adopted on the 2nd April 2009. However, because of that amendment and the "urgency" of the bill, the matter was brought before a 14 member committee (7 from Senate and 7 from Assembly) in order to produce a common text. That finalised version has been voted by the Senate on 9th April 2009, unanimously by the present senators (voting by hand). For this instance, the government of François Fillon has been accused for bringing the bill for voting very late in the evening and before Easter holidays and "grabbing" the 16 votes of the 16 present senators. However, on the same day the bill has been defeated by the national Assembly by 21 votes against and 15 in favour.

Following the defeat, and on request of the Government, the bill has been forwarded again to the National Assembly for a new lecture and on 12th May 2009 it has been adopted with 296 votes in favour and 233 against. On the very next day (13th May) the bill has been voted by the French Senate with 189 votes in favour and 14 against causing an outcry of lawyers and citizens nationally (in France) and worldwide, as well as a response by the European Parliament.

Almost immediately, the socialist party has announced its intention to contest the constitutionality of the law and on 17th May 2009 socialist MPs have submitted a request for examination to the French Constitutional Council (*Conseil constitutionnel*).

It should be noted that a few days ago, on 6th May 2009, the European Parliament had accepted an amendment (407 in favour, 57 against, 171 abstentions, European Parliament Communiqué 20090505IPR55085) to the so-called Telecommunications Package that "...no restriction may be imposed on the fundamental rights and freedoms of end users, without a prior ruling by the judicial authorities (...) save when public security is threatened...". It was actually the

second reading of the amendment that had been rejected earlier in autumn 2008 initially proposed (and rejected) as amendment No.138 by French socialist MEP Guy Bono to the distress of the French music industry. The accepted amendment No. 46 had been introduced by socialist MEP Catherine Trautman. However, following a compromise on 4th November 2009 the final wording of art. 3A of Directive 2002/21 as amended by Directive 2009/140 has made only general references to the principle of proportionality and judicial review [Broumas, 2009, Serenidis 2010, p. 194].

On 10th June 2009 the Constitutional Council has declared (Décision n° 2009-580 DC du 10 juin 2009, published in the Official Journal on the same day) the main part of the bill unconstitutional on the grounds that freedom of communication and expression deriving from the French Declaration of the Rights of the Man and of the Citizen of 1789, applies both to "*general development of the Internet*" and the "*free access of the public to internet communication services*". The decision makes particular reference to [article 9] of the 1789 Declaration conerning the presumption of innocence and [article 11] concerning freedom of expression. Furthermore, the Council has declared that the interruption of internet access may only be decided by a judge and not by an administrative authority (such as HADOPI)

On 8th July 2009 another bill, nicknamed HADOPI 2, has been presented to the French legislative chambers for the third time It has been adopted by the Senate assembly with 189 votes in favour and 142 against and in September by the Assembly with 258 votes in favour and 131 against. The bill has been again challenged by the socialist MPs in front of the Constitutional Council. However. on 22nd October 2009 the Constitutional Council has approved this new version of the law and it came into force as Law relative to the criminal protection of intellectual and artistic property over the internet (*Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet*).

### *HADOPI-2*

This "new" version of the bill characterises the interruption of internet access, up to a maximum of one year as a "supplementary sanction" (art. 7 inserting art. 335-7 to the French code of Intellectual Property) and as such it may only be imposed by a competent court according to the rules of criminal procedure; accordingly Art. 6 of HADOPI 2 modifies the French Code of Criminal Procedure to that effect. HADOPI is now limited to notify the competent criminal prosecution authorities while the main sanctions of art. 335-2 of the French Code of Intellectual Code still apply: up to 3 years imprisonment and up to €300.000 fine (5 years and €500.000 in case of organised actions). ISPs not complying with a decision to interrupt access face a fine of €5.000. Furthermore users cannot claim ignorance for third parties using their connection as the law introduces the term of characteristic negligence (négli-

gence caractérisée). If, following one year after official notification, users fail to take measures to secure their connection, then they face interruption of service up to one month. Trying to subscribe to another ISP while "suspended" may lead to a maximum fine of €3.750. It should be noted that concerns have been expressed as regards the interpretation of the extension of the criminal provisions of arts 335-2, 335-3 and 335-4 of the French Code of Intellectual Property to all types of electronic communication after the wording of Art. 6 of Law 2009-1311 "...lorsque' ils sont commis au moyen d' un service de communication au public en ligne...". This phrase could be interpreted to include emails, sms messages etc. and not only P2P file sharing, as envisaged under HADOPI-1.

## Practical constraints

the HADOPI bills have been widely criticised, as far as it concerns the violation of civil liberties, freedom of expression etc. However, before proceeding to the legal constraints in Greece, attention should be focused on the practical difficulties; the starting point is that technology should try to tackle problems caused by technology itself.

### *The number of users - the volume of data*

It is estimated that only in France offenders may be as many as 50.000 (Torrentfreak and Googlenews as of March 2010). Any judicial system, no matter how efficient, will face enormous difficulties in handling 50.000 cases. Furthermore, recent studies (University of Rennes http://www.mediafuturist.com/2010/03/foolishness-of-hadopi-2.html) reveal that between September and December 2009 (after HADOPI 2) illegal downloading of online music and video in France grew by 3%. The report shows that 30,3% of all Web users in France illegally downloaded content over the last quarter of 2009; for the period 1 July to 30 September it was 29,5%.

One possible explanation, by the same report, is that HADOPI 2 only targets P2P file sharing networks and completely ignores streaming sites. The report claims that the number of people who watch and/or download video, film and music via streaming is growing rapidly, while the numbers who do so via P2P networks is in rapid decline (Streaming media: are multimedia that are constantly received by, and normally presented to, an end-user while being delivered by a streaming provider - www.wikipedia.org). The report shows that the percentage of French Internet users who favour streaming sites rose from 12,4% to 15,8% between September and December 2009. At the same time the percentage of those using P2P networks declined from 17,1% to 14,6% over the same period. The report also indicates that those who routinely and frequently buy and download content legally, also use illegal platforms, in that sense the suspension of a connection will lead to lower legal sales and other legal activities.

Furthermore, an enormous storage space is needed to store all users transactions and normally ISPs store data in a form convenient for internal purposes; not to be used for evidential purposes by third parties. It is estimated that the storage cost can be several million euros per year, while the volume may rise up to 10.000 mails, 3.000 letters and 1.000 interruptions of service per day. The costs imposed on the state budget, as well as ISPs, will be transferred to the users leading to further barriers to the right of internet access.

### *The IP address*

It is a common understanding, that via the IP address it is very difficult to identify the actual person, which is an essential prerequisite for imposing criminal or administrative sanctions. However, even for the IP address, it is relatively easy for someone to conceal his / her identity or to impersonate another system / person either by tapping an unprotected wireless connection, or by the method of "IP *spoofing*" i.e. the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system (www.wikipedia.org). Similar problems may be born by prepaid cards for internet use, for which no contract with the ISP is required and the user may remain anonymous. Furthermore, public wi-fi hot spots allow everyone to get connected without identification i.e. user name and password. It is also common observation that many users are not accustomed with the wi-fi function of modern modem devices and do not take appropriate measures to protect their local networks. The problem becomes more complicated when members of the same group (e.g. family, workplace etc.) use the same local network via one IP address. In a manner not usual to legal texts, HADOPI bills try to sanction the owner of a connection rather than the offender him/herself.

Many commentators consider that HADOPI laws will be difficult to enforce and that there will always exist a way to circumvent the interruption of service. Finally, only "occasional" (as opposed to persistent) pirates will be persuaded by these laws to stop unlawful downloading.

## Constitutional constraints in Greece

### *Freedom of Information and Participation to the Information Society*

According to [Article 5A] of the Greek Constitution 1) All persons are entitled to information, as specified by law and 2) all persons are entitled to participate in the Information Society. The first section refers to the "freedom of information" i.e. the right to be informed. Any restrictions may only be imposed by law and if a) they are absolutely necessary and b) justified for reasons of i) national security, of ii) combating crime or of iii) protecting rights and interests of third parties. The second section

refers to the new right of participation in the information society, which is interpreted as an obligation of the state to facilitate access (not to raise barriers) for all citizens to the benefits associated with the electronic exchange of information. It has been argued that such minimal access to the Information Society has been defined by the concept of universal service [Broumas, 2009] and falls within the hard core of the right to be informed and to participate in Information Society. Consequently, we may not have restrictions beyond that minimal point of access to the service.

Under HADOPI laws, ISPs must continuously watch every transaction of the users in order to identify possible infringements. In a hypothetical Greek HADOPI law, such surveillance and consequent notification to the authorities automatically raises barriers for the satisfaction of both rights of art. 5A of the Greek Constitution: 1) Users knowing that they are under a "big brother" surveillance will reduce the use of the internet and will not feel free to visit any website they like, thus limiting the right to be informed and 2) the State does not only facilitate (as obliged) but rather raises barriers which would also contradict the principle of proportionality (see *infra*). Furthermore, it is uncertain whether the protection of IP rights may justify any of the allowed restrictions under above (i) - (iii). The brief conclusion is that such barring of users from internet use is not compatible with the Greek legal order and ECHR.

### *Data Protection And Privacy*

In Greece both the right to privacy and protection of personal date are vested with constitutional power in [arts. 9] and [9A] of the Greek Constitution, also in line with art. 6 of the Treaty of European Union, art. 8 of the Charter of Fundamental Rights of the European Union and art. 8 of the European Convention for the Protection of Human Rights.

Again, under HADOPI laws, ISPs must record and examine all user transactions, while on-line. Still, for particular cases, following an accusation from the creators of IP works, the ISP must report to HADOPI every information and data collected form the user-"suspect".

In France, the Government has asked, through the Ministry of Culture and Communication, for the opinion of CNIL (the French Data Protection and Secrecy of Communications Authority). The Committee, initially, had underlined several weak points of the HADOPI bill arguing that data surveillance should not exceed the necessary measure; that the criteria of any arbitration should be defined by presidential decree; that enforcing the law in workplaces may prove cumbersome; that private entities should not interfere with personal data for identification purposes; that freedom of expression is limited by the ISP intervention who "filters" the content; that initiating a criminal procedure by criteria defined by

private entities (the creators) may contravene the principle of proportionality; that the limits of liability between internet piracy and the control of the local private network by the user are vague; that HADOPI employees do guarantee, like the judiciary, the handling of personal data. Nevertheless, recently CNIL has given a green line for the automatic processing of IP addresses of users of P2P networks (see decision of 10-6-2010: www.pcinpact.com/actu/news/57597-orange-tmg-surveillance-cnil-p2p).

It is doubtful, following recent case law like Decisions 39/2006 and 57/2006 related to the introduction of police CCTV (see www.dpa.gr), whether the Greek Data Protection Authority, endorsed constitutionally, will consent to such general surveillance of all internet transactions by private entities such as ISPs. Still, even if we stand in front of a conflict with another right, which could justify the need to lift any protection of privacy and personal data, it is accepted, both in theory and in practice, that such conflict shall be resolved exceptionally by an *ad hoc* judgement. The end result should not affect the core of the right, leading to its annulment.

### *Freedom of expression*

Apart from other communication uses, it is well known that the Internet serves as a medium of expression; the expansion of blogs, chatrooms, messengers and social networks such as facebook, has led to an increase of the informational power of the Internet. Freedom of expression is protected under [art. 14 par. 1] of the Greek Constitution, in line with art 10 of ECHR and art. 19 of the International Covenant on Civil and Political Rights. Although art. 14 refers to expression "... *in writing and through the press*..." it is beyond doubt that such freedom also covers the Internet. In Greece this has also been verified by recent case law (see decisions 44/2008 of Court of the First Instance of Rodopi and 27/2009 of the Multimember Court of First Instance of Piraeus). The concept of "expression" covers any ideas, facts or opinions through which someone may convey and externalise his/her thoughts. In that sense any kind of message transferred over the Internet enjoys the protection provided by art. 14 of the Greek Constitution and everyone may freely form his/her opinion and communicate via any available means in written form, sounds, images etc. without any time or space restrictions. Freedom of expression may only be limited by law; however such law should not make impossible or encumber in a disproportional manner the exercise of the right i.e. should not affect the hard core of the right.

HADOPI laws are typical examples of hindrance to freedom of expression of every citizen. As a defensive right, the citizen is entitled to ask any state or private entity to abstain from any action that encumbers the exercise of the right; third parties such as ISPs are not entitled to limit the expression of ideas, the propagation of thoughts and generally the exchange of messages. Under Greek law users would be entitled to ask ISPs not to record and supervise their actions.

### *Judicial protection - Presumption of innocence*

The right of judicial protection assigns the fundamental procedural right of any person to a fair trial [arts. 8 & 20.1 of the Greek Constitution]. The principle of the "assigned" judge guarantees that justice functions independently and appoints the competent court according to institutionally established rules. Among other, the right of judicial protection covers the right of recourse to a court of law and the right to freely express in front of the court his/her opinion concerning his/her rights and interests. HADOPI -1 has been widely criticised and declared unconstitutional by the Constitutional Council, for the lack of any provision for recourse to Justice. However, HADOPI-2 has also been criticised for adopting a simplified criminal procedure in which the accused has limited rights to present his/her views (*procédure simplifiée*, see art. 6 of Law 2009-1311 inserting a new article 495-6-1 to the French Code of Criminal Procedure). It is not yet clear how [art. 3A] of Directive 2002/21 as amended by Directive 2009/1, will be interpreted in guaranteeing "*...the right to effective and timely judicial review...*", but under Greek law, any such procedure affecting fundamental rights should require a final verification through the eyes of a competent judge.

Furthermore, alleged infringers would still be convicted on the sole basis of IP addresses (see *supra*) that cannot be considered as valid evidence, and which are collected by private entities. Currently, there is no material way of opposing the validity of such "evidence", which clearly violates the presumption of innocence, a well known principle in most European legal systems (see art. 6 par. 2 ECHR), though not explicitly written in the Greek Constitution. Guiltiness of an accused must be proved by solid evidence, suspicions or doubts are not enough to convict someone in front of a court (as per known legal motto *in dubio pro reo*). Additionally, according to the HADOPI laws, the users must secure their private network and take all necessary steps to safeguard the integrity of their connection line once notified by the ISPs. Under Greek law, such action especially at the stage of initial notifications, apart from the right to judicial protection, would contravene the right to get "*a written and reasoned reply*" following a petition (art. 10 par. 1 and 3 of the Greek Constitution) and the right of a person to a prior hearing before any administrative action or measure (art. 20 par. 2 of the Greek Constitution). Applying justice by an administrative authority (under HADOPI 1) but also initiating sanctions and criminal procedure (under HADOPI 2), by the same authority or by private entities, could also raise a question of division of powers.

### *Secrecy of Communications*

According to [Art. 19 par. 1] of the Greek Constitution: "Secrecy of letters and all other forms of free correspondence or communication shall be absolutely inviolable". The right of secrecy does not have as a subject the message, already protected under

art. 14 (freedom of expression), but secrecy of communications and correspondence, no matter if it is a private or professional message. The concept of "message" covers not only written letters, but any form of communication such as phone calls, telegrams, facsimile, telex, e-mails etc., so the right of secrecy is extended to all possible means of communication. A particular independent authority has been established (Hellenic Authority for Communication Security and Privacy known as ADAE) by article 1 of the law 3115/2003, following the guidelines set in art. 19 par. 2 of the Greek Constitution; ADAE is entrusted to safeguard the right of art.19 par. 1.

There is an ongoing discussion in Greece concerning the protection of external elements of communication under secrecy (otherwise known as traffic data). Opinion 1/2005 of ADAE and Decision 79/2002 of the Greek Data Protection Authority favour protection of such data under secrecy, in line with art. 4 par. 1 of presidential Decree 47/2007, Law 3471/2006 (implementing Directive 2002/58) and law 3674/08. Directive 2006/24 for data retention, imposing stricter obligations to ISPs for the retention of traffic data, has not yet been implemented in Greece. However, opinions 7/2009 and 9/2009 issued by the Public Prosecutor of the Supreme Court argue to the contrary, claiming that traffic data are not being protected under secrecy. If we follow the Opinion of the competent authority which is ADAE, it can be argued that under Greek Law the right of secrecy covers apart from the content, also the external elements of communication, which in the case of internet include the identity and the IP of the user, the speed of connection, the place and time of connection, the duration of communication etc. Furthermore, under art. 19 par. 1 section 2, only a judicial authority shall not be bound by this secrecy and only for reasons of national security or for the purpose of investigating especially serious crimes. Law 2225/1994 has established a closed catalogue of the serious crimes for which judicial authorities may limit or cancel the right of secrecy, while investigating such crimes. It should be noted that after the *Promusicae* case (C-275/06) [detailed description in Stavridou, 2009, p. 582], recent case law of the Court of Justice of the European Union (C-557/07 *SF Gesellschaft zur Wahrnehmung von Leistungsschutzrechten v. Tele2*), takes the view that community law does not forbid member states to introduce legislation obliging holders of traffic data to reveal them to third parties (normally victims of infringement of copyright) in order to instigate civil actions based on creator's rights. Nevertheless, legislators should avoid conflicts with fundamental rights and always observe the principle of proportionality [Serenidis, 2009, p. 186].

Accordingly, it is not possible to reveal, under current Greek Law, the external elements of communication (including the IP address of the offender) unless a judicial investigation takes place for the specific crimes prescribed by law. Following the wording of the Greek Constitution (*absolute inviolable*), permission cannot be granted for a simple police search or to facilitate other administrative authorities to investigate crimes or other punishable actions that are not found in the catalogue

of serious crimes of Law 2225/94. Under the Greek Constitution we cannot have a general and preventive abolition of secrecy of communications on the Internet and in that sense, a HADOPI law would render itself in Greece obsolete, since it imposes a constant and detailed surveillance of private life and communication connected with the Internet, for actions that are not punishable as serious crimes.

### *Principle of Proportionality*

The principle of proportionality has been recognised as "generally accepted rule of law" and as a "a general rule of community law" having supranational power. In the Greek Constitution all kind of restrictions of rights "...*should respect the principle of proportionality*..." (Art. 25 par. 1 sec. c). The principle entails that between the legal purpose of a restriction and the particular restriction, there has to be a reasonable proportion. Applying the principle requires a three stage approach that of: a) appropriateness, b) necessity and c) *stricto sensu* proportionality:

a) The criterion of *appropriateness* tries to examine whether the particular measure is appropriate for the purpose. In the HADOPI scenario: Is three-strike-legislation and consequent interruption of internet access capable to fight piracy of literary works and protect intellectual property and creators? The answer is evident: Offenders could easily find other ways to communicate possibly through ISPs residing outside France. It has also been argued that through encryption methods, ISPs may not be able to recognize whether traffic of data violates IP rights.

b) If the first criterion is fulfilled the second prerequisite examines whether the particular measure is necessary i.e. if it is the mildest method between different options; otherwise it violates the principle of proportionality. Interrupting the service while the user must still pay the fee (see art. 7 of HADOPI 2) is definitely a non-necessary measure to achieve the endeavoured purpose. The purpose is to protect IP rights over the Internet; a number of milder solutions exist that lead to the same results, including technological solutions such as filtering, digital watermarks etc. Under that interpretation, the particular measure violates the principle of proportionality.

c) The third criterion is *stricto sensu* proportionality, i.e. there must be a reasonable proportion between the measure and the purpose. We have seen that a HADOPI regime in Greece would violate fundamental human rights (under 3.1 to 3.5 above); no matter how appropriate or necessary such law would finally detriment the rights of citizens in comparison to the doubtful benefits of public or private interests it is trying unsuccessfully to protect.

## Private law

a few considerations regarding private law: Under HADOPI 2 the user must still pay the monthly fee to the ISP pending the interruption of service. Furthermore,

HADOPI 2 cancels the application of the French Code of Consumers to that purpose. Under Greek Law such choice would face the following problems:

a) Taking into consideration the Greek Civil Code (arts. 380-382) in connection with the legislation for consumer protection and the contract between the ISP and the user such term should not be valid: For the period of time that the user was connected the fee has been paid and there are no further claims; for the period between the interruption of service and the end of the contract (given a limited time contract) we must establish whether the decision (judicial or administrative) to interrupt the service renders the user liable for the incapacity of the ISP to provide the service (impossibility of performance). It could be argued under art. 381 par. 1 sec. 1 of the Greek Civil Code in connection with consumer protection legislation (art. 2 of Law 2251/94), then the user may only pay compensation to the ISP, because the ISP has not yet provided the service (after the interruption) and he only has an expectation right for the duration of the contract. Any contractual term to pay the whole amount until the end of the contract would be abusive.

b) It can be argued that such provision in a Greek law would contradict the fundamental principle of freedom of contracts (Art. 361 of the Greek civil Code).

## Conclusions

Legislative proposals such as the "Sarkozy" three-strike-rule, as well as other methods for policing the Internet, raise the question whether legislators have the right to intervene to such serious restrictions concerning free access to the new universal good of communication, the Internet.

Apart from the practical constraints, we have noted that such law in Greece would be challenged by a large number of non-negligible problems related to fundamental constitutional rights, as well as by private law considerations.

HADOPI and similar laws, already introduced [Serenidis, 2010, p. 200] in New Zealand (currently withdrawn), Ireland (contractual compromise between ISP and creators), South Korea and the United Kingdom (Digital Economy Act 2010, imposing limitation or suspension of Internet Access) are the modern Circe in the Odyssey of the Internet; they try to transpose ISPs to cyberpolicemen and they try to lead the music or other IP industry to take revenge of its own audience. It looks like the only industry that believes in spying and punishing of its own clientele.

It has been supported that the IP industry should change its business model e.g. by introducing a system of remuneration, or a digital rights management system etc. and should not try to change the technology or the law. Nonetheless, before exhausting these alternatives, the IP industry should be very cautious when laying a finger on (our) fundamental rights. In our legal civilisation, law-making

still lies with legislatures and not with the industry. In the long effort to find an equilibrium between conflicting fundamental rights the players must, definitely, take into account the distinctive idiosyncrasy of Information Society.

## References

### *Greek Constitution*

**Art. 5A:** ***1.*** *All persons are entitled to information, as specified by law. Restrictions to this right may be imposed by law only insofar as they are absolutely necessary and justified for reasons of national security, of combating crime or of protecting rights and interests of third parties.* ***2.*** *All persons are entitled to participate in the Information Society. Facilitation of access to electronically handled information, as well as of the production, exchange and diffusion thereof constitutes an obligation of the State, always in observance of the guarantees of articles 9, 9A and 19.*

**Art. 8**: "*No person shall be deprived of the judge assigned to him by law against his will. Judicial committees or extraordinary courts, under any name whatsoever, shall not be constituted*"

**Art. 9.1.:** "*Every person's home is a sanctuary. The private and family life of the individual is inviolable. No home search shall be made, except when and as specified by law and always in the presence of representatives of the judicial power. 2. Violators of the preceding provision shall be punished for violating the home's asylum and for abuse of power, and shall be liable for full damages to the sufferer, as specified by law*".

**Art. 9A:** "*All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is established and operates as specified by law*"

**Art. 14.1: "***Every person may express and propagate his thoughts orally, in writing and through the press in compliance with the laws of the State*".

**Art. 19:** "***1.*** *Secrecy of letters and all other forms of free correspondence or communication shall be absolutely inviolable. The guaranties under which the judicial authority shall not be bound by this secrecy for reasons of national security or for the purpose of investigating especially serious crimes, shall be specified by law.* ***2.*** *The matters relating to the establishment, operation and powers of the independent authority ensuring the secrecy of paragraph 1 shall be specified by law.* ***3.*** *Use of evidence acquired in violation of the present article and of articles 9 and 9A is prohibited*".

**Art. 20.1** "*Every person shall be entitled to receive legal protection by the courts and may plead before them his views concerning his rights or interests, as specified by law* ". ***2.*** *The right of a person to a prior hearing also applies in any administrative action or measure adopted at the expense of his rights or interests*".

### *GREEK CIVIL CODE (Translation by C. Taliadoros, 1982)*

**381 par. 1, sec. 1**: *Impossibility of performance due to the fault of the other party. If the performance of one of the parties to a contract has become impossible due to the fault of the other party the latter shall not be freed from its obligation to furnish a counter-performance.*

### *Directive 2002/21 as amended by Directive 2009/140*

art. 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, 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.*

**French Declaration of the Rights of the Man and of the Citizen of 1789**:

**Article 9**: «*tout homme est présumé innocent jusqu'à ce qu'il ait été déclaré coupable ; qu'il en résulte qu'en principe le législateur ne saurait instituer de présomption de culpabilité en matière repressive*»

**Article 11:** «*La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme: tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi*».

Broumas A.(2009), The role of ISPs in comnnection with the application of Intellectual property Law, (in Greek), in Dikeo Meson Enimerosis & Epikinonias, 2009, p. 491

Serenidis D. (2010), Intellectual Property Infringements in Digital Networks (in Greek), Nomiki Bibliothiki, Athens, 2010.

Stavridou S. (2009), Technical measures, intellectual property and personal data (in Greek) in Chronika Idiotikou Dikeou, 2009, p. 577.

# YOUNG SCHOLARS FORUM

# Open access repositories-a perspective for the future

**Nikos Koutras**

## Introduction

Research journals on the significance and initiatives on the modern information environment have led to a significant progress in the field. The conditions of the modern information environment have evolved through the years, touching upon every social aspect of our everyday life (Bokos, 2001). Among every generation of people/end users there is a "gap" in ICTs skills, obtained through education or lifelong learning.

With the above skills one is able to fully satisfy his information needs through access to any information service. Thus, we are led to a social division between info-rich –those who have access to information- and info-poor individuals-those who are deprived of such access-, resulting to the existence of informational, and consequently social, inequalities (Papadakis, 2006).

Information Democracy, i.e. the sociopolitical system in which every person has the opportunity to profit from - access to information sources, is the only way to achieve information equality. According to Doctor, Information Democracy, as a phenomenon, empowers citizens providing them with the necessary tools and helping them learn how to use information sources that will resolve their everyday problems (Doctor, 2004).

Introducing the internet, in the 90s, has inflicted important change upon the use and accessibility to information. Several journals and editions changed their format from print to electronic and started publishing their content, a few months earlier than the printed edition, in an electronic format. As a consequence, their content became available to all registered users, limiting, at the same time, postal delay and annihilating distance by providing even home access to information.

Thus, it is clear that there is a "fertile ground" for introducing important changes to the information model through an upcoming "revolution" that could be brought through open access to information via digital repositories.

## Open Access

The idea of open access has been largely debated among the scientific community and it was turned into the "foundation stone" for a number of declarations aiming to define and promote it. The most important ones are:

## The Budapest Open Access Initiative

Published in 2002, this declaration touches upon the promotion of open access as a publication model for scientific work. It makes an appeal to institutions and scientists for publishing their entire, already evaluated, scientific work following the open access model, i.e. without any financial restrictions. At the same time, open access is characterized as "free access" to publications, offering the users the opportunity to read, download, copy, share, print, index, track and site the full text of a publication or use it for any legal purpose without financial or technical restrictions. The only prerequisite is a reference to the author and their consequent right of full control upon their publication.

This declaration proposes the two following strategies in order to achieve open access:

1. Self-archiving: This strategy will allow users to self-archive their work on the internet with the use of the necessary tools. By using the appropriate tools and following the protocols of the Open Archives Initiative, information research and retrieval through search engines will be much easier, and this means that the user will not be required to know the subject of the publication and the repository in which it was published, since this information will be provided by the search engine.
2. Open access journals: A new generation of journals, published in accordance to the open access model, should be supported and promoted. Furthermore, the existing subscriber journals should be supported and transformed into open access journals (**Budapest statement, 2002**).

## Bethesda Statement on Open Access

The Bethesda Statement on Open Access Publishing sets the basic principles for open access publishing:

A. The copyright holder grants to all users a free, irrevocable access to, and a license to copy, distribute, transmit and display the work publicly and to make and distribute derivative works in any digital medium, subject to proper attribution of authorship.
B. A complete version of the work is deposited in at least one scientifically or academically acknowledged online repository, including a copy of the copyright permission.

Furthermore, the statement offers important publishing incentives in the framework of open access, since:

- It encourages researchers to publish their work according to the principles of the open access model.
- It urges holders of cultural heritage to publish their informational sources online, granting free access to all users.
- It seeks the development of means and ways of evaluating the deposited publications in order to guarantee the repository's quality and to obtain scientific acknowledgment (Suber, 2006).

## Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities

This Declaration on Open Access to Knowledge in the Sciences and Humanities defines open access as a "comprehensive source of human knowledge and cultural heritage that has been approved by the scientific community". A basic element of this declaration is that it supports, approves and uses as a "guideline" the Budapest Open Access Initiative, the Bethesda Declaration and the European Cultural Heritage Online Center (ECHO) Charter, in order to promote the internet as a tool for the creation of an international data base of scientific knowledge and thinking, in the long run. The signatories of the declaration note that they wish to specify the guidelines/measures that research policy makers, research institutions, funding agencies, libraries, archives and museums need to consider.

The basic principle and aim of this declaration is the wide dissemination of knowledge, which is only half complete if the information is not made widely and readily available to the society. This requires a combination of the open access model and the Internet, as an ever-expanding means that provides alternative ways of knowledge dissemination.

As a consequence, there is a need, according to the declaration, for the future Web to be sustainable, interactive and transparent and its content and software tools must be openly accessible and compatible.

In conclusion, as far as the procedure that should be followed in order to include a publication in the open access model is concerned, the two basic conditions mentioned in the Bethesda statement are sited word for word (Bethesda statement, 2003).

## The Transnational Significance of Scientific Information

At this point we should mention the increasing interest of the European Union on scientific information and its use in the digital age. A communication issued on the 14th of February 2007, touches upon the access, dissemination and preserva-

tion of scientific information, in our days, all over the EU (European Committee, 2007, final).

Thus, it is obvious that access, dissemination and preservation of information have gained transnational interest that aims to the creation of a specific operational framework, which would include all these significant parameters.

This communication expressed the long term goal of the "old" continent to increase the competitiveness of knowledge economy. At the same time it aims at signaling the importance and launching a policy process on:

a) access and dissemination of scientific information, and

b) strategies for the preservation of scientific information across the Union.

The above-mentioned aim is structured around 3 pillars (European Commission, 2007, 56 final, page 2)

- The production of knowledge through research
- The dissemination of knowledge through education, and
- The application of knowledge through innovation

More specifically:

1st Pillar: All research builds on former work and depends on scientists' possibilities to access and share scientific publications and research data.

2nd Pillar: The rapid and widespread dissemination of research results can help accelerate information and avoid duplication of research efforts, and

3rd Pillar: The innovative system by which scientific information is published is pivotal for its certification and dissemination, and thus has a major impact on research funding policies and on the excellence of European research (European Commission, 2007, 56 final, page 3).

This communication comes from two policy strands, the i2010 digital libraries initiative and the Community policy on research. As far as the first is concerned, it aims at making information more accessible and usable in the digital environment. More precisely, it follows up on a letter of 26 April 2005, issued by six Heads of State and Government, asking the Commission to take the necessary steps and create methods in order to improve access to Europe's cultural and scientific heritage.

The Community policy on research aims at maximizing the socio-economic benefits of research and development for the public good. This communication represents an initial step within a wider policy process addressing how the scientific publication system operates and what impact it has on research excellence.

To sum up, it is apparent that the issue of the dissemination and preservation of scientific information presents an important challenge for the digital age at the transnational level.

## Digital Repositories

The statistical graphs of the OpenDOAR project webpage demonstrate the existing situation and the need to improve digital repositories on an international level.

## Institutional Repositories

At this point it is methodologically required to attempt a conceptualization of a fundamental category of repositories, i.e. digital repositories, by mentioning their main features, their advantages and disadvantages as well as the "cost" of obtaining information through them.

Nowadays, it is a common practice for academic institutions to create open access institutional repositories. In a first attempt to define them one could say that they are digital repositories (collections) that accumulate and preserve the intellectual products of a university or a multi-university community (Crow, 2002).

Lynch provides another quite interesting definition, according to which a digital repository is a total of services that are provided by the university to the members of its community aiming at administrating and disseminating digital objects that have been produced by university members (Lynch, 2003).

According to Ware, an institutional (academic) repository is an internet database for educational material that is scientifically approved and is characterized by duration, material accumulation, interoperability and accessibility. Furthermore, Ware notes that a fundamental aim of institutional repositories is to preserve, on a long term basis, the digital objects included in their collection (Ware, 2004).

To conclude this conceptual approach on institutional repositories and according to Crow, institutional repositories are digital collections that archive and preserve the intellectual products of a university or a multi-university community (Crow, 2002).

To sum up, institutional repositories are economical and effective projects that allow institutions to build solid relations among its scientific and research staff in order to promote scientific information.

Their content might include preprints or texts in process of writing, published articles, educational material, theses etc. Institutional repositories are accessible through the internet to all users without any cost and they guarantee a secure and proper storage of their content. They must be built according to international standards so as to be easy to use and to contain an easily indexed and retrievable content (Katsarou, 2006).

It is clear that institutional repositories provide an innovative, accessible and flexible way of obtaining scientific information.

## Institutional Repositories' Features

In her paper for the 15th Hellenic Academic Libraries Conference, G. Katsarou, specifies the main features of an institutional repository (Kastarou 2006):

- An interface through which users can submit material,
- An interface that allows content search and retrieval,
- A data base that stores content, and
- An interface for repository administrators through which they can manage and preserve the collection.

## Support Technologies and Available Software

The operability of an institutional repository is built upon the existence of the necessary hardware for the digitalization, digital processing, saving and disseminating objects through the internet. In cases where the digital material consists of old or fragile objects, the existence of specialized scanning equipment and high-definition digital cameras is required for digitization. Moreover, internet servers able to store and manage a large data volume are required (Mpanos, 2007).

As far as software is concerned there is a wide variety of digital library software packages that respond to the different needs and know-how of every university. The most popular software packages are:

- DSpace

DSpace software is an innovative digital library system that can receive, store, index and disseminate in digital form all intellectual products of universities. DSpace was created by the joint development project of M.I.T libraries and Hewlett-Packard (HP). With the creation of DSpace they aimed at building a solid, long term digital repository, which collects preserves and diffuses educational material for the research conducted by the members of the scientific community in any institution, on a local and global scale. DSpace is currently the most popular software package, since it is being used by eight Greek institutional repositories.

- CDSware

CDSware is an open-code software created by CERN in order to manage particularly large repositories that contain different types of materials, such as text, image and video. CDSware is currently being used by the Digital Collections of Modern Greek Literature and Art of the Aristotle University of Thessaloniki.

- Fedora

Fedora is a flexible software package that provides flexible tools for the management and dissemination of digital content. Fedora can be used as a basis for the development of specialized software for digital libraries and institutional repositories. Fedora is being currently used by the Pergamos Digital Library of the National and Kapodistrian University of Athens.

## Greek Open Access Institutional Repositories

At the moment there are over ten institutional repositories, either functioning or under construction, in Greek universities and Technological Education Institutes, the most important of which are:

- Anemi-Digital Library for Modern Greek Studies of the University of Crete.
- Pergamos-Digital Library of the Libraries Computer Center in the National and Kapodistrian University of Athens (EKPA).
- Psifida-Digital Library and Institutional Repository of the University of Macedonia.
- Digital Collections of Modern Greek Literature and Art of the Aristotle University of Thessaloniki.
- The University of Piraeus Digital Library.
- Nimertis-The Patras University Digital Library.
- The National Technical University of Athens Digital Library
- The Pandimos Digital Library of the Panteion University.
- Eureka-Open Access Institutional Repository of the Technological Education Institute of Thessaloniki.

Furthermore, we should mention that other digital repositories are under construction, such as the institutional repository of the Hellenic Open University (EAP).

## Conclusions

Open-access digital repositories form a political phenomenon. Politics can be examined through three different ankles: as a relation, a value or a process (Kouskouvelis, 1997). We are currently witnessing the building of a relationship among the end users and the archivists-librarians, the trainers and the trainees of university institutions and a vast variety of other organizations and institutions whishing to exchange information through digital repositories.

New values are constantly emerging, based on the open access model and digital repositories. And as Smas puts it: "in the epicenter of every European university we can now find knowledge and information…" (Smas, 2007).

The processes involved may vary and range from the methodology used up to the final integration of objects (books, magazines, scientific publications, articles etc.) to the "information tanks" of digital repositories. It is, thus, quite obvious that the future of information is based upon the wise use of technological developments. Certainly, universities are quite reluctant as far as the use of open access publications or digital repositories are concerned. This may be due to the fact that scientists and researchers are not adequately informed about the procedures followed in digital repositories.

However, as demonstrated by the abovementioned case study on Greece, there is an increasing tendency to properly operate and administrate open access digital repositories. The only way to mark progress to this direction is to constantly provide adequate information to the university administrations and the scientific and research staff in order to achieve a long term transition to this new information model.

## References

Crow Raym, 2002 "The Case for Institutional Repositories: A SPARC Position Paper", The Scholarly Publishing & Academic Resources Coalition, Washington DC http://scholarship.utm.edu/20/1/SPARC_102.pdf (viewed on 10 April, 2010)

Doctor Ronald, 1994 "Seeking equity in the national information infrastructure", Internet Research Journal, Volume 4, Issue 3, pp 9-22, MCB LUP Ltd, ISSN: 1066-2243

Lynch Clifford, 2003 "Institutional Repositories: Essential Infrastructure for Scholarship in the Digital Age", portal: Libraries and the Academy, Volume 3, Number 2, pp. 327-336, The Johns Hopkins University Press, ISSN: 1531-2542 http://www.arl.org/resources/pubs/br/br226/br226ir.shtml (viewed on 10 April, 2010)

Suber Peter, 2006 "Open Access Overview", proceedings of the 93rd Indian Science Congress, pp7-12 http://openmed.nic.in/1359/01/OA_ISC.pdf#page=8 (viewed on 15 April, 2010)

Ware Mark, 2004 "Pathfinder Research on Web-based Repositories", London, PALS (Publisher and Library/Learning Solutions) report on institutional reposi-

tories, Mark Ware Consulting Ltd. http://scigate.ncsi.iisc.ernet.in/indest-ncsi-ir/resources/PALS_report_IR.pdf (viewed on 10 April, 2010)

Communication from the Commission to the European Parliament, The Council and the European Economic and Social Committee, On Scientific Information in the Digital Age: Access, Dissemination and Preservation, COM (2007) 56 final http://ec.europa.eu/research/science-society/document_library/pdf_06/communication-022007_en.pdf (viewed on 28 April, 2010)

Zmas Aristotelis, 2007 "Globalization and Educational Policy", ed. METAIXMIO, Athens.

Katsarou Georgia, 2004 "Changing the Scientific Information Landscape with the Use of Open Access Publications and Institutional Repositories" 15th Hellenic Conference of Academic Libraries, University of Patras.

Kouskouvelis Ilias, 1997 "Introduction to Political Science and the Theory of Politics" ed. Papazisi, Athens.

Mpokos Georgios, 2001 "Introduction to Information Science", Ed. Papasotiriou, Athens.

Mpanos Evaggelos, 2007 "Greek Academic Repositories and Open Access Digital Libraries", SYNERGASIA Journal, issue 4.

Papadakis Nikos, 2006 "Towards a "Society of Skills? ed. Sakkoula, Athens.

# Peer-to-peer piracy and sociology theories – an evolution phenomenon

**Athanasios Papagiannis**

## Introduction

"Everyone has the right to be a part of the Information Society. The State is obliged to facilitate the access, production, exchange and spreading of electronically transmitted information" is the provision of article 5A, paragraph 2, of the Greek constitution, after the 2001 amendments. These amendments were a part of the huge effort to keep up with the continuously evolving technology. Sociological analysis would definitely come to the same conclusion with a systematic legal analysis: placing this provision among the fundamental human civil rights, such as the principle of equality, proves how crucial this right is for the constitutional system.

A plethora of laws, European directives and regulations exist, such as article 386A of the Greek Penal Code (fraud by means of a computer), Laws 2121/1993 and 2472/1997, which were amended by Law 3471/2006, ratified World Intellectual Property Organization Treaties, Law 2075/1992 for the foundation of the Greek National Telecommunications and Postal Services Committee, European e-privacy directive 58/2002. New authorities- national or supranational- are founded, such as the Greek independent authorities or the Body of European Regulators for Electronic Communications which, according to Manuel Castells,[1] affect very much the role of the traditional national state. Taking these facts into consideration, "expert systems", as A. Giddens described in his modernity theory, are inclined to expand even in public administration.

To be more specific, law-making process is not anymore something exclusively handled by elected- parliamentary- representatives, but it gradually turns into a "specialist team" matter[2]. These teams are supposed to compose and negotiate the normative text and submit this to the representatives. The quintessence of the normative rule usually consists of technical terminology, thus differentiating itself from common language and requiring special knowledge in order to be fully understood.

One of the situations that this kind of rules regulates is "internet piracy", which- as a socially deviant prohibited behavior- must be initially accurately described. However, at least in Greek law this word seems more to be a *convention* than a de-

finable, specific legal term, such as "fraud" or "theft". The "heart" of the Greek intellectual property legislation amended by law 2121/1993[3], which was praised[4] by Greek intellectual property institutions such as IFPI, does not contain a definition of the word piracy. Nevertheless, in article 66, a criminal punishment is provided for the unauthorized reproduction, recording, renting or selling, presentation, public distribution of audiovisual works, software, books and databases. This text contains excessively long sentences and a lot of commas, a fact that indicates how difficult was for the legislators to define this kind of criminal behavior while criminal legislation must be absolutely clear and precise (the "nullum crimen nulla poena sine lege stricta et certa" principle). On the other hand, article 370C of the Greek Penal Code is much simpler and far more specific in its subject. It focuses on unauthorized copying or usage of software. In this essay, we will use the following definition of internet piracy: "temporary or permanent, free of charge, acquisition or offer of copyrighted digitized audiovisual works, software, through an open and accessible computer network".

This subject is quite complicated and its analysis would lead to further questions that sometimes are not closely related to sociology. However, it is one of the key aspects of digital technology revolution in the post industrial society [5] and a part of its identity. Any approach to this matter without a brief- at least sociological-analysis of the technologies that made it possible, would be deficient and maybe inappropriate for the information era.

## Technology: an unpredictably evolving revolution

The creation of the internet itself could be considered a latent function[6] of united states military institution. During the cold war era, when Soviet Union launched the "Sputnik", military organization required rapid and effective radar communications. It was initially covered by the ARPANET[7] university network, which was later commodified and offered as a service open to the public. Its spread would reach even 100% per year[8]. According to Douglas Comer[9], the internet's decentralized structure and lack of- profit oriented- copyright patents in communication protocols are to thank for this quick spread.

The lack of monetary profit-oriented structures was one of the main aspects of the Napster service. It was one of the first online free file sharing services which set a milestone for the phenomenon called online piracy. Yet, this service did not last long. Technology-wise it was a major innovation and- regarding its judicial evaluation- it is mentioned in every modern Intellectual Property book as the predecessor of modern peer-to-peer systems. It was a technological breakthrough due to the fact that its network was based on a totally different structure in comparison with the conventional networks. Instead of relying on a costly central

computer-server, which would certainly have some specific functional limitations, it diverted the workload to many client computers offloading the master server. Users did not need to download the files from the server. The server would transmit them some information regarding the location of the file across the internet. Then, the client user would download it from another client and would re-upload it to another user. This innovation, which as a concept is similar to the decentralization of political power in political science, was called "Peer-to-Peer". Its effectivity was enormous. In March 2001, Napster users were estimated to be around thirty million[10]. However, the Records Industry Association of America (RIAA) filed a lawsuit[11], which after the verdict of the court of appeal resulted in the takedown of this service and a 36 million dollar fine that napster would try to earn by the commercial use of its service. This effort was not fruitful and napster was bought by American company Best Buy for 121 million dollars[12].

Another major innovation was the Bittorrent protocol, invented by Bram Cohen and distributed for free since July 2001[13]. Although it is a peer-to-peer protocol too, it can be much more effective as it is even more decentralized and it relies on the fragmentation of the files into chunks, a fact that makes their partial transfer possible, thus making the whole network even more independent from the server's availability. Its distinctive feature is the "userbase" dependence: Its high effectivity is correlated with its users' cooperation. If the users stop offering their files for download (also known as seeding), the network will stop functioning[14]. Furthermore, downloading speeds, also known as network throughput, depend on the amount of seeders for each file. No user is allowed to download a file without offering his own files for uploading. Although- according to informatics' science- such a network model would seem non viable 8 years after its invention and data exchanged with the bittorrent protocol across the internet worldwide account for 55% of overall traffic[15]. Yet, since this protocol is a part of the peer-to-peer network evolution, the main part of this data is copyrighted material (pirated copies). The scientific capital of this invention was transformed into monetary capital. In 2004, the inventor founded the Bittorrent Incorporated digital media distribution company, which would later be funded by Doll Capital Mangement, and after a contract with Motion Pictures association of America would ban any form of pirated material from its search engine[16].

It is obvious that the internet as a military means of communication, was an autopoietic system [17] in the beginning but then was commodified. After the hi-tech business corporations, such as Information Technology corporations, whose profit stems from a high level of know how and specialization, a new, quite productive young[18] *élite* was born. This *élite*, thanks to the available technology, engages its productivity and innovation in order to create something perhaps not vital but useful, and offer it to society for free. Contrary to modern capitalism, this elite

is not after profit itself, but its main motive is knowledge and offer to society. Despite the usage of enthusiast-created peer-to-peer networks being illegal, internet users often choose to ignore this manufactured risk[19], depending on their respective country tolerance towards piracy[20]. On the other side, there are multinational corporations where the main motive is profit per se and this profit is endangered by piracy. Due to that fact, they attempt to assimilate these networks by investing on them and adapting them to their own production model. As an example we could refer to Blizzard software company which distributes its programms through bittorrent networks. As we saw in the Napster and Bittorrent case, the main institutional reaction to an illegal activity will not be a lawsuit or a legal action but a financial transaction that will lead to the acquisition of the deviant entity by an investor willing to adapt this entity into a pure capitalist production model.

Furthermore, the character of this revolution is not just financial or technological but it also consists of a social aspect. Belgian digital society anthropology professor Michel Bauwens structured a new sociological paradigm, the Peer-to-Peer theory, which can be quite useful regarding an analysis of the piracy phenomenon.

## Peer-to-Peer theory and internet piracy

This theory is based upon the assumption that the protestant-Calvinist ethics, upon which modern capitalism was based according to Max Weber[21], was gradually altered and exacerbated. According to peer-to-peer theory[22], piracy is only a part of the peer-to-peer phenomenon. Open source software is another aspect of the same phenomenon. This theory can also rationalize the "piracy ethics". In the modern socioeconomic system, cognitive capitalism, maximum profit is possible through innovation and knowledge, therefore more through immaterial than not material means. This is a concept similar to Manuel Castells' informationalism[23]. We live in the post-Fordism era, and the nature of work is heavily altered. The Worker is not anymore a part of the machine, supposed to carry out a simplified-predefined task as soon as possible but a creative unique individual, expected to engage his full subjectivit, in Michel Bauwens' words.

This kind of worker, called knowledge worker by McKenzie Wark[24] although appearing in various forms such as artists, graphic designers, programmers, managers, has some certain characteristics: a) immaterial object of work, b) sophisticated and specialist, c) high stress, time sensitive work, d) high use value. This use value is converted to commercial, monetary value through the social class Bauwens and Wark call vectoralists. This class is in control of the immaterial flows[25] between knowledge work and consumer society, thus being a successor to industrial capitalism capitalist class. To be more specific, industrial capitalists made profit

by controlling the means of production which were material and not accessible to wide public. Nowadays, computers and electronic devices that dominate the production procedure are not financially unreachable but it is practically impossible for a consumer to buy all available software, which is a major profit source for the IT industry. It is clear that Karl Marx's social class theory can be quite helpful in understanding Bauwens and Wark theories which can support an argument against Bell's situses theory[26]. Bell argues that conflicts are not anymore among social classes in the post industrial society. They are horizontal instead. Vectoralists' profits depend on knowledge workers productivity.

However, since the knowledge workers work results into immaterial objects such as software, and the main dimension of modernity according to A. Giddens is space being disembedded by time, knowledge workers work can be rapidly reproduced and multiplied anywhere. Bauwens argues that there is an abundance when it comes to knowledge work, which is the opposite of scarcity that endangers only physical objects, such as natural resources, and every economy branch relying on them, such as industry. This abundance does not fit in our modern neoliberalist, hypercapitalis, social system, where everything is subject to commodification. The only way for the vectoralists to sustain their profits is to induce an artificial scarcity of knowledge goods through pushing towards the direction of a stricter more prohibitive intellectual property-copyright legislation, since the peer-to-peer networks can always produce use value without demanding the consumption of a respective exchange (monetary) value. This theoretical analysis is rather close to Karl Marx's theory about law's function as rules oriented towards the financial interests of the dominant social class- vectoralists- who will oppose to any effort of the knowledge workers class to achieve the maximum possible- legal or illegal- access to knowledge works, the fruit of the labours of their own class.

At this point, a new question arises. How did the knowledge workers manage to gain so much power that they can pose a threat for the vectoral class which is assumed to be socially superior to them? Using the peer-to-peer scientific paradigm the answer- in Bauwens words- would be something like "new social dynamics, which are already a social fact and rapidly spread across society, peer-to-peer dynamics". This theory's asset is its individuality: it does not attempt to oversimplify using abstract theories but is much more precise. Bauwens also uses isomorphism[27] as an effective analytical tool. If some certain structures obviously share some similarities, then there will probably be other, not so obvious, similarities or analogies in these structures.

Peer-to-Peer networks and communities developing around them are a suitable example. Although the innovator of this theory distincts between decentralized and distributed networks, there are some common principles. If workload and

authority are distributed across equipotent user and obligatory duty turns into community-oriented contribution, a certain system becomes much more effective and flexible from a profit oriented structure/system. Keeping in mind the previously mentioned peer-to-peer networks functions, we could easily draw parallels with political decentralization. The same way a computer network does not depend anymore exclusively on servers reliability and effectivity, modern states public structures shift e.g. to flexible independent authorities, more open to the citizens, thus solving problems such as red tape. It is a matter of overall social change.

The term equipotent is also of major importance. The innovator of the theory, in video interview[28], argues that peer-to-peer systems, despite their highly specialised nature, are totally anticredentialis, participation is open and proccess-free, noone has to prove his level of expertise or demonstrate some certain abilities. Entering a peer-to-peer network does not require a certain symbolic capital[29]. They are not what Anthony Giddens would call expert systems either, they offer deinstitutionalised knowledge instead. This openness is crucial in comprehending their role, bearing in mind the fact that Microsoft Corporation, whose dominance in Operating Systems market is undisputable, gained the position that it holds today by successfully marketing since 1995, a Graphic User Interface computer operating system[30], and simplifying computer's use by eliminating the need for command-line interfaces.

Another aspect of Peer-to-peer systems is the nature of the motives. The basic motivation is not financial profit or outperforming all competitors. Contribution in the form of participation is totally voluntary- there are no obligatory activities. The main motivation is the best possible result per se. This could sound similar to Karl Marx's theory, since "everyone offers according to his ability and expects to receive according to his needs". According to Bauwens analysis, Peer-to-peer systems superiority lies in their motives: System-wise, instead of being extrinsic, they are intrinsic. A peer-to-peer community will not download movies/music/software to gain some kind of financial profit but his main goal is movies/music/software itself, which he will later share with the rest community members. The activity is a goal in itself, it is not a medium for achieving something else. From a structural -functionalist point of view, according to Talcot Parsons and Robert Merton theories[31], this characteristic covers the need for a latent status and non-financial social values. To be more specific, this system maintains the value of cooperative work [32] because it relies on cooperative human nature instead of relying on competitive human nature. The more it develops, the firmer its base becomes. Even in everyday language, this kind of networks resuscitated the meaning of the words "community", "commons", and bearing in mind the fact

that peer-to-peer support websites call themselves communities, we can easily understand the functions of such groups.

But how do these communities are administrated? That is one of the reasons why peer-to-peer systems can be superior than other social models. There is a demonopolization of power instead of standard authority-control structures. There is no pyramid-like hierarchy, but some symbolic indicators[33], which serve as an evaluation and intrinsic quasi reward of each users contribution. As an example we could refer to the ratio indicator found in bittorrent protocol. It indicates the amount of data offered-uploaded relative to the data received-downloaded by the user and it is a part of his-her identity in a specific peer-to-peer community, as it is usually printed next to his nickname. New users, with ratio less than 1:1, do not have full user access, while users with a relatively low ratio are called leechers in a degrading manner and sometimes banned from the communities. Some other communities use the reputation system which incorporates a more complicated way of evaluating users contributions', based on how frequently they contribute or how effective their advice towards other members are. Sometimes, positive evaluation leads to elevated (administrator) user rights such as the authority to control misbehaving users. In both cases, evaluation is always dynamic instead of static. Hierarchy structures are not fixed and there are equal chances for everyone, which seems to be a major asset compared to modern political systems, where election requires public relationships and funding[34.] In addition to that, peer-to-peer systems sustain a totally intrinsic motivation. Evaluation is symbolic and cannot be used anywhere except for the network. Although it may seem meaningless, the majority of peer-to-peer users are keen on contributing more and more to their networks. Many of them maintain a second, low-end home computer in order to upload files all day long. So peer-to-peer systems development is organic[35] and autonomous, without central administration or dependence, thus proving the superiority of a non profit model compared to a scientifically structured profit driven corporate model such as the vectoralist company model.

## Peer-to-Peer Piracy in modern culture

Piracy- as a social phenomenon- and the reaction to it, be it prosecution or legalization is obvious in our modern culture. There is a plethora of caricatures, tv spots and controversial texts around the internet. To begin with, the Motion Pictures Association of America's advertisment[36] in the beginning of every DVD movie attempts to classify piracy as theft of a material object. This advertisment remains unchanged since the video cassette era, being rather unable to keep up with the current evolution. This rather "demonizing" approach is even more frequent and direct in the previous decade's anti-piracy advertisments[37]. The crimi-

nal system symbol is used in a rather extreme and disproportionate way, by depicting a person being arrested in front of a mother and a child. The same symbol is used in a picture where a professor is arrested during class and two students share the reward. However, these pictures are rather hard to find, but all this is easy to explain: intellectual property interested corporations have been forced to change their public relations policies and ameliorate their messages by appealing users morality after realizing the power of peer-to-peer networks.

Peer-to-peer networks wide spread is an argument often used by their users. In picture [44], there is an other MPAA ad reminding that tracing a person committing piracy is technically possible with the message "you can click, but you cannot hide". Pirates response is "you can sue but you cannot catch everyone", indicating a rather collective- or perhaps community oriented- way of thinking. The meaning of this message is of major importance: it is based on the assumption that the definition of a crime as a deviant behavior must be a society-oriented concept. In pirate's opinion, when a behavior is adopted by the majority, it should stop being classified as a deviant behavior because reality should have a certain normative role in social life.

In another picture[38] modern law is criticized in a quite interesting way, too. In picture [38], under the title "Piracy is not theft. A handy guide, theft, removes the original, piracy makes a copy", the willingly childish and handmade looking picture attempts to clarify the distinction between material and intellectual property. For a person who is not aware of the respective legislation, the terms "property" or "ownership" are equal to the meaning of the ancient Roman legal term "dominium". Therefore, an average person cannot comprehend the ratio legis for criminalizing unauthorized copying and considers respective legislation to be rather unfair. Another picture[39] uses childish sketches and compares file sharing with piracy. Sharing is depicted as a rather happy picture where two smiling persons share a toy. Piracy is depicted as a murder committed by the first person in order to keep the toy for herself. Compared to pictures[37], where a virtual violation of the principle of proportionality occurs, the roles are inverted. The vectoralist corporations are heavily criticized on the grounds of disproportionate reaction to piracy. In peer-to-peer users opinion, vectoralists act as if piracy was murder. Taking a second look into picture[39], we will notice that the victim is an African American woman. It is a hint on *Capitol v Thomas* case, which took place in Minessota, US, in 2007 and a retrial in 2009. The defendant, anative American and mother of four children, was found liable for infringing 24 songs via the peer-to-peer Kazaa network and was ordered to pay $1.920.000 in statutory damages, later reduced to $54.000[40]. Those indirectly expressed arguments are mixed in video[41], where the message of video[36] is ridiculed by a comparison with the kidnapping of a baby. In the end of this video, police invades a house and

shoots a person who downloads pirated material dead. This is a rough picture of what peer-to-peer users think about intellectual property legislation and its enforcement. They think that their fundamental rights, such as the right of privacy, are disproportionally endangered by legislation tailored to suit *vectoralist* corporations profitability, since they do not accept any intervention to their privacy no matter what this certain privacy conceals.

In another picture[42], a much more sophisticated communication technique is used and a more complicated message is created. Under the title "When you pirate MP3s you are downloading communism", a smiling fiend in former Union of Soviet Socialist Republics officer uniform stands behind a person using an iMac computer. The message style is the same as a second world war Allied picture with the title "When you ride alone you are riding with Hitler", which was used in the US during the second world war to support the fuel economy campaign. So, this picture criticizes the methods that the intellectual property rightholders use to fight piracy, by drawing the parallels with war propaganda. However, peer-to-peer paradigm shares some concepts with the communist theory. On the other hand, peer-to-peer piracy as a phenomenon is totally incompatible with modern social-economic model, and it can definitely bring some groundbreaking changes. These changes pose a threat to vectoralist corporations market share and profits, and according to the picture, that is the reason why these corporations try to demonize piracy in a way which resembles to cold-war era methods. According to these corporations, piracy is a threat for the American dream itself. We should also notice the kind of computer the user operates in this picture. Apple computers are one of the top selling, lifestyle consumer goods, and their success relies on their ease of use and style, contrary to less stylish, yet cheaper, IBM compatibles. It is implied that piracy is a capitalist system phenomenon which evolved uncontrollably and now threatens the essence of capitalism, financial profit.

## Conclusion

Technological evolution had a huge impact on various fields, such as law, science and sociology. It has altered them but there are always some substantial needs, such as adequate rights theories, when it comes to privacy in internet communications. However, the peer-to-peer paradigm offers an analytical tool capable of contributing to the comprehension of peer-to-peer related phenomena, such as the Zopa private bank.

In addition to that, peer-to-peer piracy has an influence on politics, too. Although piracy is illegal, there are already some parties whose goal is its legalization, along with changes in copyright legislation and stricter communications privacy legislation. This has began in Sweden in 2006, where a certain incident trig-

gered a shift towards such parties. After the Swedish Police arrested the owners of the famous Pirate Bay torrent tracker, the members of the Swedish pirate party doubled in two days. It was not a coincidence. After the verdict in 2009, three thousand additional members joined the party in three hours. One week after that, this party had 40.000 members total[43]. Similar developments occur in other countries too showing an effort to institutionalize a currently illegal behavior.

## Endnotes

1. It is the fourth dimension of the "Information Age".
2. As an example, we could refer to the Greek parliament regulation: Articles 160-162A provide for the special scientist service, which is also referred to in article 65 paragraph 5 of the Greek constitution. In the European Union's institutions, the Committee is capable of founding small specialist groups. This has been criticized by the European parliament with the 19.1.1993 resolution.
3. This law was used to ratify EU copyright directives such as 91/250, 2001/29, 2004/48.
4. http://www.ifpi.gr/mission/piracy2b.htm IFPI considered this law to be innovative and, according to it, what matters is not the law by itself but its enforcement.
5. Daniel Bell "The coming of post-industrial society", Basic Books Inc. Harper 1973.
6. I. Lambiris- Dimakis "Sociology and its methods", vol A.2003, Sakkoulas, page 63, Robert K. Merton theory.
7. http://www.darpa.mil/history.html Defense Advanced Research Projects Agency History accessed 27.5.2010.
8. http://www.dtc.umn.edu/~odlyzko/doc/internet.size.pdf 1998 Koffman, K. G; Odlyzko, A. M. The size and growth rate of the Internet. AT&T Labs accessed 27.5.2010.
9. Comer, Douglas (2006). The Internet book. Prentice Hall. p. 64.
10. http://en.wikipedia.org/wiki/File:Napster_Unique_Users.svg according to this chart, accessed 27.5.2010.
11. *A&M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896 (N.D. Cal. 2000) 239 F.3d 1004 (9th Cir. 2001).
12. http://paidcontent.org/article/419-breaking-best-buy-to-acquire-napster-for-121-million/.
13. http://finance.groups.yahoo.com/group/decentralization/message/3160 inventor of this protocol announces its distribution, accessed 27.5.2010.
14. This network concept would be a total failure in a commercial, failsafe high availability network, such as a hospital or a bank network. This kind of networks relies on traditional server-client structures.
15. http://www.ipoque.com/resources/internet-studies/internet-study-2008_2009 Ipoque company research.
16. http://www.zeropaid.com/news/5952/mpaa_bit_torrent_reach_agreement/ accessed 27.5.2010.
17. Term used by Niklas Luhmann in "Systemtheorie, Evolutionstheorie und Kommunikationstheorie", (1975), in Soziologische Gids 22 3. pp.154–168.

18. Shawn fanning invented napster when he was 19 years old and bram cohen created the bittorrent when he was 26 years old.
19. Ulrich Beck's Terminology, Ulrich Beck, Risk Society, Towards a New Modernity, Sage 1999.
20. http://www.nationmaster.com/graph/cri_sof_pir_rat-crime-software-piracy-rate 2007 accessed 27.5.2010.
21. Max Weber, Die Protestantische Ethik Und Der Geist Des Kapitalismus 1905 in http://www.marxists.org/reference/archive/weber/protestant-ethic/index.htm accessed 27.5.2010.
22. http://integralvisioning.org/article.php?story=p2ptheory1 2005 accessed 27.5.2010.
23. Castells, The Rise of the Network Society The Information Age: Economy, Society and Culture Vol. I. Cambridge, MA; Oxford, UK: Blackwell(1996) .
24. McKenzie Wark, Hacker Manifesto Harvard University Press, Cambridge, 2004.
25. Castells, The Rise of the Network Society The Information Age: Economy, Society and Culture Vol. I. Cambridge, MA; Oxford, UK: Blackwell (1996).
26. Tatsis N.H. Modernity and Social change, Nissos 2004, p. 177.
27. This term is also familiar in biology, math, chemistry and IT.
28. http://video.google.com.au/videoplay?docid=4549818267592301968&hl=en-AU# accessed 27.5.2010.
29. Term from Bourdieu, Pierre (1984) Distinction: A Social Critique of the Judgement of Taste. London: Routledge.
30. It is the now widespread Windows graphic Operating System.
31. Parsons, The Structure of Social Action, Free Press, Second edition 1967.
32. Perhaps this sounds too optimistic, but I think it is a quickly spreading trend in our times. It can be found on electronic entertainment, where multiplayer, nstead of single-player, online games conquer the market.
33. Tatsis N.H. Modernity and Social change Nissos Publications 2004, page 78, "Anthony Giddens".
34. This is called full inclusion system by M. Bauwens.
35. Term coined by Alexander Galloway in his book "Protocol" How Control Exists After Decentralization MIT Press, 2004.
36. video found in http://www.youtube.com/watch?v=iPcHhOBd-hI&NR=1 accessed 27.5.2010.
37. http://worldofstuart.excellentcontent.com/antipiracy.htm accessed 27.5.2010.
38. http://questioncopyright.org/piracy_is_not_theft accessed 5.10.2010.
39. http://www.blackgate.net/images/sharing_is_not_piracy.png accessed 5.10.2010.
40. http://www.webcitation.org/5n2E7HM3z January 22,2010 accessed 27.5.2010.
41. http://www.youtube.com/watch?v=ALZZx1xmAzg accessed 27.5.2010.
42. picture in http://tiny.cc/na9mg accessed 5.10.2010.
43. http://en.wikipedia.org/wiki/Pirate_Party_(Sweden) accessed 27.5.2010.
44. http://tiny.cc/2naqy and http://tiny.cc/ocgb4 accessed 5.10.2010.

# Freedom of art as freedom of expression in modern times

Freedom is walk the way your talents show you, Henri Matisse

**Maria Spyrou**

## The Principle of the Constitutionally Guaranteed Freedom of Art

The principle of the constitutionally guaranteed freedom of art is based on the German Constitution of Weimar Republic in 1919. In particular, in Article 142, paragraph 1, it is defined that:

Art, Science, as well as teaching of Art and Science, are free. The State provides protection and participates in their development.

The ultimate goal is the advancement of the personality of the individual in all aspects –social, political, spiritual, and of course artistic ones.[1]

Unfortunately, it was not long before the most hideous censorship considering the plastic works of the European art took place in the very same country that defended freedom of art constitutionally. Although the Constitution was not officially abolished, the rise of the National Socialist Party under the leadership of Hitler labeled modern art in various ways, one of which was called "Degenerate Art" (Entartete Kunst). On 10th July 1939, 730 works of art of prominent artists were exhibited in an anti-exhibition in Munich. The organizers of the anti-exhibition altered the works of art before the latters were "burned at stake".

As a result, the "victims" of the European art by the end of the World War II amounted to 70,000 works of art, while a lot of artists were forced to flee from Germany. The ones that remained in Germany were deprived of the right to free expression and creativity[2]. The infringement of the personality of the individual along with the encroachment of property was part of the ideological background of the Nazis, which had as a result the infringement of art.

## Freedom of Art in Greece

In Greece, freedom of art was constitutionally guaranteed for the first time in 1925 and 1927. Then, in the revised Constitution of 1975[3], clause 16, paragraph 1 defines that:

Art, Science, Research, and Teaching are free; the state is obliged to develop and advance them. Academic freedom, as well as the freedom of teaching, does not stand over the obligation to abide by the Constitution[4].

We should not fail to mention two very important points in the above mentioned definition. The first one has to do with the definition of art. The Constitution does not give a priori any kind of definition of art, may it be a general or a special one.

The second one is the constitutional foundation of art, which links the production of the works of art with their presentation to the public[5]. It is obvious that, based on the Constitution, the ultimate goal of art is communication and there is no mention whatsoever about "art for art".

In addition, Article 5, paragraph 1, of the Constitution defines that:

All persons shall have the right to develop freely their personality and to participate in the social, economic and political life of the country, insofar as they do not infringe the rights of others or violate the Constitution and the good usages [6].

According to the legislator, all citizens are free to express their personalities up to the point they do not infringe the rights of others. It is obvious that the above mentioned definition is advantageous for the status quo, in contrast to the minorities that may exist. We should not fail to mention that the above mentioned clause is not only restricting but also inconsistent to Article 16, paragraph 1[7]. Furthermore, according to the legislator, good usages are referred to applied moral concepts, which are defined by the law within the limits of the Constitution[8].

Moreover, Article 14, paragraph 1, of the Constitution defines that:

Every person may express and propagate his thoughts orally, in writing and through the press in compliance with the laws of the State.

What is more, Law 1291/1982 paragraph 3 establishes the freedom of speech in the works of art and science, stating that the characterism obscene cannot be applied to them[9].

## Art and Censorship

The etymology of the Greek word for art "τέχνη" goes back to the verb "τίκτω", which means the humans' ability to create[10]. Besides, it is expressed in various ways, which leads to the conclusion that there are many kinds of art, according to the feelings that are expressed though them, i.e. theatrical arts, the art of poetry, the seventh art, plastic arts etc.

The fact that there is no particular definition for art, from the very first time art appeared in our lives until today, is to be attributed to the sui generis nature of art. It is common knowledge that the question concerning the concept of art has troubled all the people that, one way or another, are linked to art: plastic artists, philosophers, art historians, critics, as well as those who produce and defend cultural politics.

Most aesthetic theories that have been developed until today with a view to examining the concept of art refer to the two basic philosophical trends:

According to Plato, art is the imitation of real nature (transcendental forms)[11]. On the contrary, Aristotle suggested that art had cognitive value, i.e. an ultimate goal. Examining tragedy in particular, he defined that goal as the catharsis of the soul[12]. All philosophical theories, despite their different approaches, converge to the primary need of the individual to express their personalities through various forms of art. Artistic creation is the fruit of this expression as an action of thought on the issues people have to face, particularly the ones referred to their deeper emotions. Emotions such as rage and anger, sorrow and loneliness, expectation and joy, trigger human imagination creating images that people feel the need to express.

However, what can be considered extreme in artistic creation leading to the censorship of a work of art? Up to which point is art free?

Censorship of art is not something new; there have been numerous cases in the past. Without doubt, the first audience of a work of art is its creator. According to the theory of receiving, a work of art is not a formed entity but in the course of time it receives new concepts and explanations. What today is considered extreme by the public opinion, insulting our personalities, in the future it may not only be acceptable but also the landmark of an art movement. Besides, modern art does not aim at depicting natural beauty but rather truth, subjective truth, since it is common knowledge that there is not only one and absolute truth.

However, what happens when the artistic creation derives from personal desperation or from a will to be provocative?

In order to give an answer to these questions, we should examine the era of the French revolution between 1830-1848, when people read daily newspapers to learn what was happening in the country. This is the era when art critique is prominent. As Charles Baudelaire stated: “Critique! The fact that an artist is pretending to be important so easily happens because the critic is without doubt one of the many[13]. Even though this was stated so much time ago, these words seem to apply to the current situation. Art is said to generate culture, which in turn ennobles the soul. In some occasions, plastic works of art communicate with

the audience by provoking or by shocking. In that way it seems that the artistic creation is deprived of any kind of invention, in which case art is only the echo of these voices that serve aesthetics, of these voices that consider art as a means of impressing and achieving economic and personal goals.

## Endnotes

1. See Theodosis, 2000: 17-18.
2. See Charalampidis, A. 2002:119-128 V. II. One freedom of art in relation to photography see Bottis, 2009.
3. It should be noted that the Greek Constitution was also revised in 1986 and 2001.
4. See the website http://lawdb.intrasoftnet.com/nomos/2_nomothesia_artl_current.php (accessed at: 15.06.2010) http://lawdb.intrasoftnet.com/nomos/2_nomothesia_artl_current.php (accessed at:15.06.2010).
5. See Dagtoglou, 2005: 738 V. A.
6. See the website: http://lawdb.intrasoftnet.com/nomos/2_nomothesia_artl_current.php.
7. See Theodosis: op. cit., p. 81.
8. See Dagtoglou, 2005: 1339, V. B.
9. See in detail Law 5060/ 1931 paragraph 30 as replaced by Law 1291/1982 paragraph 3.

http://lawdb.intrasoftnet.com/nomos/2_nomothesia_artl_current.php (accessed at:20.06.2010).

10. See Pelegrinis, 2009: 618.
11. See Scouteropoulos, 2003: 708-716.
12. See Beardsley, 1989: 47-52.
13. See Baudelaire, 2005: 25.

## References

Bottis M., Right to a photography and right to personality, in Stamatoudi I. (ed.), Journalists and Publishers and mass media Sakkoulas, 2009, pp. 232-262 (in Greek).

Dagtoglou P. D., (2005) Constitutional Law – Human Rights. Athens: Sakkoulas Publications V. A & B (1st edition: 1991).

Theodosis, G., (2000) Freedom of Art. Athens: Kastaniotis Publications.

Pelegrinis, Th., (2009) Dictionary of Philosophy. Athens: Ellinika Grammata Publications (1st edition: 2004).

Scouteropoulos, N. M., (2003) The Plato Republic. Athens: Polis Publications (1st edition: 2002)

Charalampidis A., (2002) The Art of the 20th Century. Painting – Plastic Arts – Architecture in the Interwar Period. Thessaloniki: University Studio Press Publications, V. II (1st edition: 1993)

Baudelaire C., (2005) Aesthetic Essays. Ed. Tsikoudis, A. Athens: Printa Publications (1st edition: 1995)

Beardsley C.M., (1989) History of the Aesthetical Movements. Athens: Nefeli Publications.