TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Social Sciences
Tallinn Law School

Tommi Sundqvist

Analysis of the European Regulatory Framework on ePrivacy. Implications of Emerging Technologies in ICT

Master Thesis

Supervisor: Katrin Merike Nyman-Metcalf, LL.M, Ph.D

Tallinn 2015

I hereby declare that I am the sole author
of this Master Thesis and it has
not been presented to any other
university of examination.

Tommi Sundqvist
“ ..... “ 2015

The Master Thesis meets the established requirements

Supervisor Katrin Merike Nyman-Metcalf
“ ..... “ 2015

Accepted for examination “ ..... “ 2015

Board of Examiners of Law Master’s Theses

……

Table of Contents

Abbreviations

CI – Critical Infrastructure

CIIP – Critical Information Infrastructure Protection

CJEU –The Court of Justice of the European Union

DPA – The Data Protection Authority

EDPS – The European Data Protection Supervisor

ePrivacy – Privacy in the online context, includes but is not limited to data protection.

ECHR – The European Convention on Human Rights

ECtHR – The European Court of Human Rights

EPO – The European Patent Office

GPI – Global Patent Index

ICT – Information and Communication Technology

IETF – Internet Engineering Task Force

IPC – International Patent Classification

ISP – Internet Service Provider

NRA – The National Regulatory Authority

OECD – The Organisation for Economic Co-operation and Development

PbD – Privacy by design

PETs – Privacy Enhancing Technologies

PPP – Public-Private-Partnership

WIPO – The World Intellectual Property Organization

W3C – World Wide Web Consortium

A. Introduction

Technologies have been opposed and blamed in various times in different contexts throughout history of mankind, and quite often seen threatening the individuals' right to privacy. In addition to Luddites as an obvious example, there is an even more intriguing example. As Plato once wrote, Theuth, the inventor of numbers and writing, once presented his inventions to Pharaoh, among those the invention of writing as the recipe for memory and wisdom. Against all expectations Pharaoh was genuinely unsatisfied. He understood the new invention of writing in existing context through lenses coloured by old ideology and judged that invention will have harm on those who employ it since external memory necessarily substitutes the training of memory i.e. thinking.[1]

All new technologies, to be more precise, real or perceived consequences of new technologies from numbers to Information and Communication Technologies (ICT) have been tried to repudiate or allow, to hinder or to foster by regulation. One obvious way of doing this is to introduce new specific laws on emerging technologies sometimes leading to proliferation of *sui generis* regulation. It can be argued that this is partly due to genuine necessity, partly due to the lack of interdisciplinary understanding of technologies – understanding that technology does not substitute, but more likely complements and fosters thinking. Understanding unique technologies[2] would provide capacity to interpret existing law or to introduce new regulation to achieve the objectives such as protecting the right to ePrivacy.

Pace of technological progress and emerging technologies in ICT present challenges to law never seen before. In 1890 Warren and Brandeis in the *Right to Privacy* referred to the next step which must be taken for the protection of the person.[3] One of the earliest definitions of privacy was given by Judge Thomas Cooley who defined privacy as the right to be left alone, “The right of privacy, conceding it to exist, is a purely personal one, that is, it is a right of each individual to be

1 Plato, Euthyphro, Apology, Crito, Phaedo, Phaedrus (1914)

2 Technology can be understood in a conceptual level e.g. eTechnologies, or as a specific technology *e.g.* solution for some existing problem. In this thesis, technology is understood in the conceptual level if not clearly otherwise expressed e.g. by words 'specific', 'unique' etc.

3 S.Warren & L. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, at 195 (1890) [The Right to Privacy]

let alone, or not to be dragged into publicity."[4]

Since then privacy has become an even more multifaceted concept. Considering the developments in the society such as the convergence of the physical and virtual world, and the penetration of technology in all corners of our life – both public and private, privacy and data protection has become the focal point where all ideologies and aspects converge i.e. center of interest and activity. The Parliamentary Assembly of the Council of Europe suggested in 2011 that the epochal progress in ICT challenges the right to privacy and data protection and they need to be protected by legislation, "In a democratic state governed by the rule of law, cyberspace must not be regarded as a space where the law, in particular that concerning human rights, does not apply."[5]

Technology, law and privacy interactively shape how we define and undersand them. Privacy revolves around issues such as private communication and self dignity, and data protection around issues such as the processing of personal data. The difference between privacy and data protection in ICT stems from the idea that data protection concentrates on data, privacy on the more fundamental rights of the individual.[6] Nevertheless privacy is the starting point for considering data protection. Hence this thesis discusses ICT implications from the privacy perspective and the term ePrivacy is used to define the privacy in ICT context in digital world including data protection.

I. Problem Field

Developments on privacy, ICT and law lay down the problem field for the thesis. Technology cannot be understood only as a specific tool or mean which needs to be regulated. This necessarily invokes new requirements in understanding the law. The technology side of for

4 Classification of legal rights *in* T. Cooley, A Treatise on the Law of Torts. Or the Wrongs which Arise Independently of Contract 364 (1906) [Classification of legal rights]

5 *See* Parliamentary Assembly resolution 1843. The protection of privacy and personal data on the internet and online media. Council of Europe (2011) Available: http://assembly.coe.int/ASP/XRef/X2H-DW-XSL.asp?fileid=18039&lang=EN Accessed: 25.10.2014

6 *See, e.g.*, S. Gutwirth, R. Leenes & P. De Hert (Eds.), European Data Protection: Coming of Age (2013)

example e-Governnance is not the problem area, but to make emerging technologies fit into the existing regulatory context in the course of *inter alia* introducing successful government eServices certainly is. In this sense, the current European regulatory framework on ePrivacy related issues in ICT should be analyzed and possible challenges identified.

By studying the academic literature and research regarding the same problem field from two different angles, existing literature in law related to technology and literature in technology related to law, two major gaps can be identified. There is a clear gap in the research on social implications of technology. Another gap is in the legal research to understand specific emerging technologies to identify the implications on right to privacy in European legal context.

Relevant research does exist in the field of law and technology considering aforementioned problems, but research combining both practical data on emerging technologies and legal research methods to analyze regulatory framework from purely legal prespective certainly provides new information to the existing research field.

II. Scope of the Thesis

The scope of the thesis is ePrivacy related legislation in the European regulatory framework. Scope is limited to emerging information and communication technologies (ICT) using the taxonomy of the International Patent Classification (IPC) proposed by the OECD.[7]

The analysis of national legislation is outside of the scope of this thesis.

III. Objective of the Thesis

The objective of the thesis is to analyze how current European legislation responds to certain threats or risks to privacy in digital world.[8] This is done by first identifying the implications of

7 *See*, International Patent Application Guide (2014) Available: http://www.wipo.int/export/sites/www/classifications/ipc/en/guide/guide_ipc.pdf Accessed: 16.12.2014

8 The threat is understood as a capability and intent, whereas the risk as a probability and harm, which may also actualize without clear intention by being only 'in the wrong place at the wrong time'.

specific emerging technologies in ICT on privacy. Main challenges are identified and recommendations made on how the European regulatory framework should be developed to better respond to new ePrivacy concerns.

Other objective is to assess whether patents are an adequate and suitable source of data for legal research. It is assessed whether based on patent indicators relevant emerging technologies in ICT can be selected, and furthermore new threats to ePrivacy identified.

It must be noted that the research question on whether patents are a valid source of data is symmetrical in the way that positive and negative findings will add to the knowledge.

The objective is not to identify or make predictions on what the most successful emerging technologies in ICT are. Nor is it to analyze how regulatory framework affects emergence and implementation of technologies i.e. legal constraints on ICT, although the thesis may provide some answers to these questions.

IV. Hypotheses

Hypothesis of the thesis is that emerging technologies in ICT introduce totally new requirements for European regulation including legislation on privacy and data protection. Although, only due to the convergence of physical and virtual world and rapid development of emerging technologies there is no inherent requirement for parallel law, but on specific issues, such as processing of sensitive personal data, the equal level of privacy to be achieved in the digital world compared to physical world might need additional protective measures and stronger response.

Furthermore, supportive hypothesis is that complexity of regulation, however good and necessary single laws may be, reduces the efficacy of the regulatory framework.

The second supportive hypothesis is that the overregulation i.e. red tape in EU terminology, is a probable risk that stems from the complex nature of existing regulation as well as from lack of interdisciplinary approach.

Instead of formal regulation, a) coherent and absorbing ICT regulation in ePrivacy related issues

should be preferred, and b) the solutions specific for ePrivacy related issues in ICT can be found from innovative sources *inter alia* from other areas of law, from other disciplines or from technology itself.

V. Research Questions

- Are patents an adequate and suitable source of information for analyzing privacy issues regarding ICT in the future from the legal perspective?
- Based on research on ICT patents, what are the most significant implications emerging technologies in ICT have on ePrivacy?
- How does the current European Regulatory Framework for ICT respond to new ePrivacy threats?
- Can a general approach on how to respond to privacy threats be recommended by analyzing specific implications of emerging technologies?

VI. Prior Art

1. Existing Academic Legal Literature on Law and Technology

The relation between law and technology has long been studied in jurisprudence as well as in more practical legal analysis. Although Europe is currently recognized as a global leader in regulating eTechnologies as well as in promoting fundamental rights, in the early 20th century U.S. was predominant in considering privacy related issues from the legal perspective.

One of the landmark cases in privacy is *Olmsted v. United States* in 1928,[9] where Court Justice Brandeis argued for a constitutional right to privacy and identified the impact of new technologies on law in relation to privacy by noting that although wiretapping was designed to

9 *Olmstead et al. v. United States; Green et al. v. United States; McInnis v. United States*, 277 U.S. 438 (Sup.Ct. 1928)

protect against crime, the over-extension of the new technology could lead to an environment that is less secure.

In the late 20th century Laurence H. Tribe created the general theory of law and technology focusing on the future impacts of an emergent technology in a conceptual level.[10]

One of the more modern researchers studying the interrelation between law and technology is Harvard Law Professor Lawrence Lessig. In a book *Code and Other Laws of Cyberspace* in 1999, he argued that computer code may regulate conduct in internet in a very similar way how legal code does.[11] It can be seen to be written in opposition to the notion that cyberspace and internet could not be regulated.

The Advocate General at the Court of Justice of the European Union, Juliane Kokott, and her Legal Secretary Christoph Sobotta, studied privacy and data protection from the European legal perspective by analyzing the distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR.[12]

Lyria Bennet Moses studies the pacing problems and analyzes *inter alia* technological change and proliferation of *sui generis* legal rules.[13] Several other publications can be found studying the relation between privacy and technology with a more philosophical approach,[14] as well as using jurisprudential methods.[15] Several legal analysts consider how law can best protect interests and values when they are threatened by technological developments.[16] In addition, sociological research exist studying the role of technology in social systems and capitalism.[17]

Current research touches upon topics such as how ICT can help in understanding law by

10 L. Tribe, *Technology Assessment and the Fourth Discontinuity: The Limits of Instrumental Rationality,* 46 S. Cal. L. Rev 617, (1973)
11 L. Lessig, Code and other laws of cyberspace (1999)
12 J. Kokott, & C. Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR,* 3 IDPL 222, (2013) [Privacy and data protection in the CJEU and ECtHR]
13 L. Moses, *Sui Generis Rules in* G. Marchant, B. Allenby & J. Heckert (Eds.), The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem, 77 (2011) [Sui Generis Rules]
14 L. Austin, *Privacy and the Question of Technology, 22* Law and Philosophy 119 (2003)
15 D. Solowe, M., Rotenberg & P. Schwarz, Privacy, Information and Technology (2006)
16 *See, e.g.,* A. Cockfield, *Transforming the Internet into a Taxable Forum: A Case Study in E-Commerce Taxation*, 85 Minn. L. Rev 1171 (2001) discussing on situations where technological change challenges traditional tax policy principles.
17 *See, e.g*., A. Giddens, The consequences of modernity (1990) and M. Weber, The Protestant Ethic and the Spirit of Capitalism (1930)

simplifying it,[18] as well as how information technology is introduced to regulatory policy-making,[19] and how ICT can help enhancing privacy protection.[20] Also possibilities of computerized legal structuring has been studied recently.[21]

During the last few years the legal research has undergone significant changes due to the profound change in legal information. A traditional researcher relied on a set of law books and established sources, whilst the new generation does not rely on libraries but databases and sources on the internet. However, the most pivotal change identified in the legal research is not in habits how research is conducted, but on how we think about the law.[22]

In legal research there are several studies that try to analyze practical implications of technology on concepts such as privacy.[23] Although, these studies operate with top-down methods not using practical data available. There is also recent research on privacy enhancing technologies (PETs) that sees privacy not merely as an individual right, but as a public good which needs to be protected by technological tools such as data obfuscation and creating online pseudonyms.[24]

Most recent research is on regulating eTechnologies in European Union considering legal aspects of cybersecurity and eGovernance.[25]

---

18 K. Nyman-Metcalf & E. Täks, *Simplifying the law—can ICT help us?*, 21 Int J Law Info Tech 239 (2013)

19 *See* C. Coglianese, *Information Technology and Regulatory Policy: New Directions for Digital Government Research*, 22 SSCR 85 (2004)

20 *See* A. Rull, E. Täks & A. Norta, *Towards Software-Agent Enhanced Privacy Protection, in* Protection in T. Kerikäe (Ed.), Regulating eTechnologies in the European Union, 73 (2014) for discussion on the ability to control the use of personal information as a part of the right to privacy, and how software agents can be used for this purpose.

21 E. Täks & A. Lohk, *An alternative method for computerized legal text restructurin*g Proceedings of the 2010 conference on Legal Knowledge and Information Systems: JURIX 2010: The Twenty-Third Annual Conference, 171 (2010)

22 R. Berring, *Legal Research and the World of Thinkable Thoughts*, 2 J. App. Prac. & Process 305 (2000)

23 *See* B-J. Koops, & R. Leenes, *Privacy regulation cannot be hardcored. A critical comment on the 'Privacy by design' provision in data-protection law,* 28 IJLIT 159 (2014) for analysis on the Draft General Data Protection Regulation and 'privacy by design' provision.

24 *See* Z. Kwecka *et al*. *"I am Spartacus": privacy enhancing technologies, collaborative obfuscation and privacy as a public good,* 22 Artiff Intell Law 113 (2014) for more information on PETs and especially on data obfuscation as a tool.

25 T. Kerikmäe, (Ed.) Regulating eTechnologies In the European Union: Normative Realities and Trends (2014) [Regulating eTechnologies in EU]

2. Other Relevant Academic Literature

Studies have focused on identifying the relationships between information and communication technologies based on patent citation analysis on the ICT sector.[26] The multiple classifications of patents have been used to analyze the impacts and future changes in the technology, but they are limited in not utilizing empirical data.[27] Research on which patent indicator offers 'best fit' in correlation with other science and technology indicators are conducted by using empirical information gathering methods *inter alia* random sampling of the *Official Gazette of the US Patent and Trademark Office.*[28]

The processing of intellectual property documents, such as patents, has been important to the economists and business communities. Recently also legal academic research has recognized its possibilities.[29] One significant trend has been the studies identifying legal constrains on new technologies and on more general fields of technology.[30]

In addition the technologies addressing the 'privacy problem' are studied both in a very practical,[31] as well as on a theoretical level.[32] Substantial amount of research and studies have concentrated on biotechnology and pharmaceutical sectors,[33] but very recently in rising numbers on new emerging technologies and technological concepts in ICT such as cloud computing.[34]

---

26 In F. Narin, *Patent bibliometrics,* 30 Scientometrics 144 (1994) it is noted that frequency that a patent is cited in subsequent patents reflects the impact of its technological innovation and the pervasiveness of its technological information. The number of citations per patent represents both the quantitative frequency and the qualitative importance of that particular patent.

27 *See, e.g.,* C. Changwoo, K. Seungkyum & P. Yongtae, *A patent-based cross impact analysis for quantitative estimation of technological impact: The case of information and communication technology,* 74 Technol Forecast Soc 1296 (2007)

28 J. Frame & X.Tong, *Measuring national technological performance with patent claims data*, 23 Res Policy 133 (1994)

29 A. Fujii, M. Iwayama & N. Kando, *Introduction to the special issue on patent processing,* 43 Inform Process Manag 1149 (2007)

30 *See* M. Niemelä & O. Pitkänen, *Privacy and data protection in Emerging RFID-Applications*. EU RFID Forum 2007 (2007)

31 M. Madejski, M. Johnson & M. Bellovin, The Failure of Online Social Network Privacy Settings (2011)

32 S. Gürses, Multilateral Privacy Requirements Analysis in Online Social Networks. PhD thesis, KU Leuven (2010)

33 C. Prins, *Biometric technology law, Making our body identify for us: Legal implications of biometric technologies,*14 CLSR 159 (1998)

34 S. Pearson & A. Benameur, *Privacy, security and trust issues arising from cloud computing,* Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010, 693-702 (2010)

VII. Organization of the Thesis

The first Chapter 'A. Introduction' lays the reason behind selecting the topic for the thesis and presents the scope and hypotheses of the thesis. The objectives and research questions are introduced. The overview on related research is also provided in 'VI. Prior Art'. Finally the research methods are explained, validity and reliability assessed, and relevance and contribution to the existing research considered.

Chapter 'B. Regulatory Framework' reviews the regulatory framework including European primary and secondary law as well as relevant case-law related to different aspects of ePrivacy in ICT. Also international primary law is presented.

In chapter 'C. Emerging ePrivacy Implications – Patents as a Source' the patent research is conducted and its findings are presented.

In the Chapter 'D. Discussions' the European regulatory framework is analyzed based on the findings of the research. Discussion is divided into two self-standing entities: 'I. Past Ideology' and 'II. Present Law'.

The aim of the first Part 'I. Past Ideology' is to position the ePrivacy related issues into the historical perspective and understand the continuously changing features of the privacy concept in ICT. The relationship of technology and law from the privacy perspective is considered in a theoretical level.

Second Part 'II. Present Law' mirrors the found implications of research to existing legal context and discusses the privacy issues of emerging technologies in ICT from a strictly legal perspective and with legal research tools. In this part the emphasis is not on constraints law imposes to emerging technologies as such, but to consider the European regulatory framework for ICT to identify possible weaknesses considering the future development, thus chapter contributes to the conclusions and recommendations on how the legislation should be revised or interpreted for best efficacy resulting in best protection of ePrivacy.

The fifth Chapter 'E. Conclusions and Recommendations' presents the main conclusions of the thesis. This chapter serves as the main contribution of the thesis providing general recommendations how to respond to new implications of emerging ICT in regards to ePrivacy.

VIII. Research Methods

Legal research methods are used such as scholarly articles; published academic books; primary and secondary law; as well as case-law. Yet, if research is conducted using only legal research tools, the interdisciplinary academic legal thesis[35] in the field of law and technology is hardly inventive and may lack in explanatory value. In order to identify emerging technologies as future-oriented, yet the most relevant as possible, patent database proved to be suitable source of data.

Simple taxonomy of patent classification created reliable, accessible tool to identify the most significant fields of ICT from which patent documentation for qualitative analysis were selected. To identify emerging technologies in ICT, the WIPO PATENTSCOPE and EPO PATSTAT databases were used.[36] In the first step, the most relevant patent classes in ICT were identified based on two indicators, the total amount of relevant patent applications in IPC sub-classes and the growth rate.[37] In the second step, to select the specific ICT patents from identified most relevant ICT classes, database queries were conducted. The queries were made by using technology related terms from the *EJLT* article topics published in year 2012 and 2013, [38] as well as by identifying relevant terms from European Commissions Digital Agenda for Europe web pages.[39]

The qualitative method used for identifying new privacy implications was document analysis which was conducted manually. Findings from different patents were analyzed subjectively to assess what the main implications are based on the claims and descriptive parts of the patent documentation.

Based on results, analysis of the European regulatory framework for ICT on ePrivacy was

35 S*ee, e.g.,* J. Kerper, *Creative Problem Solving vs. the Case Method: A Marvelous Adventure in which Winnie-the-Pooh Meets Mrs. Palsgraf*, 43 Cal. W. L. Rev 351 (1998)
36 Source for EP data is DOCDB, EPO master documentation database.
37 J. Lawrence, A Catalog of Special Plane Curves (1972)
38 The European Journal of Law and Technology archive including 2012 and 2013 volumes available in http://ejlt.org/issue/archive Accessed: 15.12.2014
39 *See* http://ec.europa.eu/digital-agenda/en Accessed: 15.12.2014

conducted by traditional legal research methods studying *inter alia* European Union primary and secondary law as well as CJEU and ECtHR case-law.

1. Validity and Reliability

Although several methods were used, the benefit is that similar research can be conducted in other fields using statistical variables,[40] qualitative document analysis and legal research methods.

Data is available also for other fields than ICT, easily accessible, possible to re-test and publicly available. Yet, the presented results are considered in the defined context, and at specific point in time hence they are not as such to be understood to be scalable or provide conclusions to be used in other context.

The value of the patent databases from which primary data was collected lies in the fact that it is a new yet easily comprehensible complementary source and the assumption is that in legal research it is used in addition to other sources of information. It also provided simple measure to identify what are relevant technologies. In that sense, it was mainly to be tested, whether there are patent variables found that can be used to identify technologies.[41]

The found implications can be considered valuable, since based on them, it was possible to find implications of emerging technologies and further to study the European regulatory framework. Also what data was used, how it was collected, and based on which criteria selected can be clearly presented.

IX. Relevance and Contribution to the Existing Research

When studying the emerging technologies in ICT, conventional methods such as case-law,

40 L. Given, The Sage encyclopedia of qualitative research methods (2008)

41 The patent applications and patent grants as variables are publicly available due to the requirement of disclosure and are clear in what they measure. They are input variables to measure invention activities in technologies that are patentable according to certain agreed rules such as inventiveness and industrial applicability that is measured by patent office in process of patent examination.

opinions, works of legal scholars, legislation, and other commonly accepted jurisprudencial sources are used to analyze the regulatory framework. But to find new ePrivacy implications that emerging technologies introduce, the source of data to identify these implications has to be novel or source not previously used for the same purpose.

The conducted patent research contributes to the existing research by providing information that was collected uniquely for this thesis. Patents serve as an adequate tool for narrowing the scope of the thesis to concern only ICT.[42] In addition, all specialists, practitioners and researchers can adopt the patent variables used to their research method 'toolkit'.

Technological change nor legal evolution occurs in a vacuum, but in an almost symbiotic connection with other fields of society. Regulating technology is a complex task, not only because of the technology itself, but the fact that the aspects of 'emergence' and 'new' as well as 'context' present legal challenges. The legislation regarding data protection is one of the most relevant and under constant change in the European Union law. Considering the current revision of existing regulation *inter alia* proposal for new general data protection regulation; attempts to regulate cyberspace; new concepts and principles such as right to be forgotten: privacy by design; digital divide; the Big Data; digital single market; and eGovernance there are areas of law that are yet not fully discovered and new ones emerging. Hence there is also demand for new ideas combining the best features of law and technology to contribute to the existing research.

42 *See*, International Patent Application Guide (2014) Available: http://www.wipo.int/export/sites/www/classifications/ipc/en/guide/guide_ipc.pdf Accessed: 16.12.2014

B. Regulatory Framework

In this chapter the European regulatory framework for ICT is reviewed. Primary focus is on legislation governing privacy in the digital world i.e. ePrivacy. The case-law regarding several aspects of ePrivacy by European Court of Human Rights (ECtHR) and Court of Justice of the European Union (CJEU) is presented.

The areas of law that may touch upon issues related to ePrivacy, such as family law, commercial law, competition law and intellectual property law are not considered.

I. EU Primary Law

1. Background

The Council of Europe was formed in the aftermath of the World War II to promote the rule of law, democracy and human rights. For this purpose, it adopted the European Convention on Human Rights in 1950, which entered into force in 1953. The European Court of Human Rights (ECtHR) was set up in 1959 to ensure that contracting parties fulfil their obligations.[43]

The European Convention on Human Rights was an international agreement between the 47 States of the Council of Europe. It is not primary law of the European Union, yet all member states of the EU are contracting states of this agreement.[44]

It would be very difficult to translate the right to privacy into precise legal terms, hence it was

43 In the system as first set up, three institutions were given the task of ensuring compliance: the European Commission of Human Rights, the European Court of Human Rights and the Committee of Ministers of the Council of Europe. With the entry into force of Protocol No. 11 in 1998 the first two institutions were merged into a single Court. *See, e.g.,* A. Zervaki, Resetting the Political Culture Agenda: From Polis to International Organization. Springer Briefs in Law, 41-43 (2014)

44 The accession of the European Union is currently under negotiation, see the Final report to the CDDH, Fifth Negotiation Meeting Between the CDDH Ad Hoc Negotiation Group and the European Commission on the Accession of the European Union to the European Convention on Human Rights, Council of Europe (2013) Available: http://www.coe.int/t/dghl/standardsetting/hrpolicy/Accession/Meeting_reports/47_1%282013%29008rev2_EN.pdf Accessed: 18.12.2014

mentioned in *Travaux Préparatoires* to the Convention, that Convention "could lay down a general rule, leaving the exceptions thereto and the methods of application to the legislation of each contracting State."[45] The general prohibition of interference with the right of privacy means in practice that there is no list of possible legal grounds for interference, but ECHR concentrates on the necessity of legal basis.[46]

Before the Charter of Fundamental Rights of the European Union came legally binding, fundamental rights as general principles of EU law were mostly protected by the Convention.[47] Thus, the Convention and Charter are closely aligned.[48] Both the Convention and the Charter of Fundamental Rights have a provision on privacy. The right to respect private life in Article 8 of the Convention is subsequently protected in Article 7 of the Charter providing that everyone has the right to respect for his or her private and family life, home, and communications.[49]

Another Article 8, namely Article 8 of the Charter, specifically addresses the fundamental right to the protection of personal data which origin can be seen in another Convention of the Council of Europe, the Convention 108 i.e. Data Protection Convention.[50]

2. Charter of Fundamental Rights of the European Union

The original treaties of the European Communities did not contain any reference to human

---

45 Preparatory Work on Article 8 of the European Convention on Human Rights. European Commission of Human Rights, Council of Europe, 10 (1956) Available: http://www.echr.coe.int/Documents/Library_TravPrep_Table_ENG.pdf Accessed: 26.11.2014

46 'Private life' was used as a synonym for 'privacy' in ECHR, *see* O. Diggelmann & M. Cleis, *How the Right to Privacy Became a Human Right,* 14 Human Rights Law Review 441, at 457 (2014)

47 *See* J. Kokott & C. Sobotta, *The Charter of Fundamental Rights of the European Union after Lisbon* EUI Working Papers, 1 (2010) Available: http://cadmus.eui.eu/bitstream/handle/1814/15208/AEL_WP_2010_06.pdf?sequence=3 Accessed: 18.12.2014.

48 Privacy and data protection in the CJEU and ECtHR, supra note 12

49 *See* para. 23 *in Case C-62/90 Commission of the European Communities v Federal Republic of Germany*, [1992] EU:C:1992:169

50 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe (1981) can be seen actual and relevant considering for example current reform in data protection regulation, especially relating the concept of 'sensitive data' since Article 6 of the Convention 108 covers special categories of data such as personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life or criminal convictions.

rights, but in year 2000 the European Union proclaimed the Charter of Fundamental Rights of the European Union which sets out civil, political, economic and social rights divided into six sections including dignity, freedoms, equality, solidarity, citizens' rights and justice.[51] Charter applies to institutions and bodies of European Union's national bodies when they adopt a national law implementing an EU directive or apply an EU regulation.

The Charter guarantees the respect for private and family life in Article 7, and establishes the right to data protection in Article 8. Article 8 provides that personal data must be processed "on the basis of the consent of the person concerned or some other legitimate basis laid down by law" embodying the pre-existing EU data protection law.[52]

Since the Lisbon Treaty entered into force in December 2009, the European Union Charter of Fundamental Rights enjoys the same legal value as the Treaties as an EU primary law meaning that Charter became a legally binding instrument.[53]

II. EU Secondary Law

The so called second generation of legislation considers the protection of personal data separate from the right to privacy. The accelerating developments in ICT and the rising role of information and threats stemming from the new possibilities to use i.e. process the data gave 'right to data protection' its *raison d'être* in the European regulatory framework. The secondary law hence considers privacy in very ICT relevant context.[54]

---

51 European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, 20 (2014) [Handbook on European data protection law]

52 *See* Art. 8 of the Charter of Fundamental Rights of the European Union, OJ 2012 C326/391 [The Charter of Fundamental Rights of the European Union]

53 Art. 6 of TEU reads: "The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties." For legal binding *See, e.g.* Press release *European Commission swears oath to respect the EU Treaties,* European Commission (2010) Available: http://europa.eu/rapid/press-release_IP-10-487_en.htm Accessed: 12.12.2014

54 *See* Chapter 4 'The future of online privacy and data protection' *in* Van Eecke *et al*., Legal analysis of a Single Market for the Information Society (SMART 2007/0037) (2009)

1. Data Protection Directive 95/46/EC and Data Protection Regulation 45/2001

The first and principal European Union legal instrument on data protection is 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,[55] which was adopted by the European Union designed to protect the privacy and personal data of citizens of the EU, but also to advance the free flow of data in EU.[56]

In time of its adoption in 1995, several member states had already adopted national data protection laws. It can be derived from this fact that the aim of adopting the Data Protection Directive was to reconcile and harmonize the data protection laws that had evolved at the national level to create minimum level of protection.[57] Although, in *joined cases 468/10 Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* and *469/10 Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado,* [2011] EU:C:2011:777, Court held that "the harmonisation of those national laws is not limited to minimal harmonisation but amounts to harmonisation which is generally complete."[58]

Personal data in the context of Data Protection Directive is defined as "any information relating to an identified or identifiable natural person".[59] For the practical implications on ICT, the data such as address, geo-location, time of online purchase or credit card numbers can be considered personal when the information can be identifiable directly, or indirectly to a specific person. Sensitive personal data such as health or ethnic origin in the context of the Data Protection Directive is conditional to free and informed consent of the data subject.[60]

The processing of personal data "mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording,

55 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. OJ 1995 L281/31 [Data Protection Directive (1995)]

56 Handbook on European data protection law, supra note 51

57 Recitals 1, 4, 7, 8 of Data Protection Directive (1995), supra note 55

58 Paras. 28-29 *in joined cases C-468/10 Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and C-469/10 Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado* [2011]

59 Data Protection Directive (1995), supra note 55, Art. 2(a)

60 Data Protection Directive (1995), supra note 55 *See* Art. 8 for special categories of data. For further considerations, it can be argued that even name of the individual can reveal racial or ethnic origin.

organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".[61]

The Data protection rules apply when controller is established or operates within European Union, but what is notable, as Article 4(1)c stipulates,[62] it applies also when the controller uses equipment located inside the EU to process personal data. This means that controllers such as search engine operators from outside the EU must also comply with this directive, thus the directive has an international effect.

Article 7 of the Directive[63] requires that personal data shall only be processed if at least one of six legal grounds listed in that Article apply. Criteria list for making data processing legitimate include, *inter alia*, that the data subject has unambiguously given his consent; processing is necessary in order to protect the vital interests of the data subject; and processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article1(1).[64]

As Article 29 Data Protection Working Party notes,[65] the balancing test provided in Article 7(f) should not be treated as 'a last resort' where other grounds for legitimate processing are deemed not to apply or automatically chosen either.[66] Yet, what ultimately constitutes a legitimate interest has been interpreted differently across member states since it is for the member state to implement the Directive under their national laws.

As the Data Protection Directive could address only member states, an additional legal instrument was created to establish data protection for the processing of personal data by institutions and bodies of the EU, namely EU Institutions Data Protection Regulation No.

---

61 Data Protection Directive (1995), supra note 55, Art. 2(b)
62 Data Protection Directive (1995), supra note 55
63 Data Protection Directive (1995), supra note 55
64 Data Protection Directive (1995), supra note 55, Art. 7 (a), (d), (f).
65 Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Art. 30 of Directive 95/46/EC and Art. 15 of Directive 2002/58/EC
66 *See* Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Article 29 Data Protection Working Party, 9 (2014)

45/2001.[67]

2. ePrivacy Directive 2002/58/EC and Commission Regulation No 611/2013

In areas already partially covered by the Data Protection Directive 95/46/EC,[68] ePrivacy 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,[69] provided more detailed data protection provisions regarding electronic communication sector, and applies also to legal persons.[70]

ePrivacy Directive sets out rules on how providers of electronic communication services, such as telecommunication companies and Internet Service Providers (ISPs) should manage their subscribers' data. Directive sets out rules on *inter alia* risk of breach of security requiring network providers to take appropriate technical and organisational measures to safeguard security of its services in Article 4(2);[71] confidentiality of communications over public networks by prohibiting the listening into, tapping and storage of communications without the consent of the users concerned in Article 5; security of networks and services; traffic and location data by requiring data be erased or made anonymous when no longer required for communication or billing purposes, except if the subscriber has given consent for another use in Article 6 and 9; and data breach notifications in case of breach of security that leads to personal data being lost or stolen.[72] Article 5(3) of the ePrivacy Directive requires that, to store or access to information stored on a user's computer, tablet, mobile phone or any comparable equipment used for accessing the internet, clear and comprehensive information is given about the purposes of the processing.[73]

---

67 Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ 2001 L 8/1

68 Data Protection Directive (1995), supra note 55

69 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L201/37 [ePrivacy Directive 2002]

70 Handbook on European data protection law, supra note 51

71 R. Wong, Data Security Breaches and Privacy in Europe, 10 (2013) [Data Security Breaches and Privacy in Europe]

72 Id.

73 Id.

Finally, some adjustments were made to ensure consistent implementation of the data breach rules across member states and the Commission regulated the measures applicable to the notification of personal data breaches.[74]

3. ePrivacy Directive 2009/136/EC

In 2009 the European Parliament adopted an amendment, Directive 2009/136/EC, to the 2002/58/EC ePrivacy Directive and 2002/22/EC Universal Service Directive.[75] Among other modifications the new version of the Directive changed the provisions about the use of cookies and similar technologies and introduced an obligation for website operators to receive their users' consent.[76] In other words, in addition to condition of 'providing clear and comprehensive information' in Article 5(3) of the 2002/58/EC user's consent is required before the use of cookies and similar technologies.[77] This is also the reason why Directive is sometimes referred to as a 'Cookie Directive'.

Directive guarantees also the access to services of the disabled end-users' to the same level as other end-user i.e. same functionality and usability of services by different means[78]; and regarding implementation and enforcement, for member states to lay down rules on penalties including criminal sanctions and ensure competent national authority with power to obtain any relevant information they might need to monitor and enforce national provisions adopted.[79]

---

74 Regulation 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications. OJ 2013 L173/2 [Regulation on notification of personal data breaches 2013]

75 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ 2009 L337/11 [ePrivacy 2009 amendment]

76 Id., art. 2, amendment to art. 5(3)

77 *See* Article 29 Working Party Opinion 04/2012 on Cookie Consent Exemption. 7 June 2012. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf Accessed: 22.10.2014.

78 Id., *see* Recital 12 of the Directive for amendment to Directive 2002/22/EC (Universal Service Directive), which can be understood as providing means that are not necessary equal but equitable.

79 Id., *see* inserted Art. 15(a) to Directive 2002/58/EC (Directive on privacy and electronic communications)

4. The European Regulatory Framework for Electronic Communications

The European Union regulatory framework for electronic communications is a series of rules which even in *bona fide* can be said to be quite complex to navigate through, although the objective was to establish harmonized framework. In 1999 European Commission initiated the first review of existing ICT law which resulted in the adoption of a new regulatory framework for electronic communications in 2002. In second round in 2009 the regulatory framework was amended.[80]

The Telecommunication package consists of The Framework Directive 2002/21/EC [81] amended by Better Law-making Directive 2009/140/EC [82] and Directive 2009/136/EC on citizen's rights concerning the processing of personal data and the protection of privacy,[83] Regulation 1211/2009 creating the Body of European Regulators for Electronic Communications (BEREC) and its Office[84] in 2009, and four specific directives Access Directive[85]; Authorization Directive[86];

80 Handbook on European data protection law, supra note 51

81 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 OJ 2002 L108/33

82 Directive 2009/140/EC Of The European Parliament And Of The Council Of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services OJ 2009 L 337/37

83 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws OJ 2009 337/11

84 Regulation 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office OJ 2009 L337/210

85 Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities OJ 2002 L337/37

86 Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services OJ 2002 L108/21

Universal Service Directive[87]; and Directive on Privacy and Electronic Communications[88], as well as Decision on radio spectrum policy.[89]

The Directive on Privacy and Electronic Communications[90] concerns the processing of personal data and the protection of privacy in the electronic communications sector. Article 4 of the Directive concerns security, Article 5 confidentiality, Article 6 traffic data, Article 8 presentation and restriction of calling and connected line identification; Article 9 location and other data; and Article 14 technical features and standardisation. Directive provides member states possibility to adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3), (4), and Article 9. Directive was amended by new ePrivacy Directive 2009/136/EC in 2009.

5. eSignature Directive and eIDAS Regulation

The purpose of eSignature Directive 1999/93/EC is to facilitate the use of electronic signatures and to contribute to their legal recognition by providing a legal framework for electronic signatures and certain certification-services for cross-border transactions.[91] The Directive essentially covers electronic signatures. Regarding other aspects of data protection, member states must ensure that certification service providers and national bodies responsible for accreditation or supervision comply with other relevant regulation in force, e.g. Directive 95/46/EC on the protection of personal data. [92]

In order to ensure the security and legal validity of an electronic transaction in cross-border

87 Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services OJ 2002 L108/51

88 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 OJ 2002 L201/37 [Directive on privacy and electronic communications]

89 Decision 676/2002 of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community OJ 2002 L108/1

90 Directive on privacy and electronic communications, supra note 88

91 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures OJ 2000 L13/12 [eSignature Directive 1999]

92 Data Protection Directive (1995), supra note 55

operations, it is pointed out by European Commission that legal certainty is needed.[93] Hence the new regulation was proposed in 2012[94] which encompasses *inter alia* time stamping, i.e. the date and time on an electronic document which proves that the document existed at a point-in-time and that it has not changed since then; and electronic seal, i.e. the electronic equivalent of a seal or stamp which is applied on a document to guarantee its origin and integrity.[95]

The member states had not embraced the eSignature Directive as much as wished, and lack of trust made consumers, businesses and administrations reluctant to carry out transactions electronically and to adopt new services.[96] After the eIDAS Regulation 910/2014/EC was adopted on 23 July 2014, and more precisely, after the adoption of relevant implementing acts member states may voluntarily recognize notified e-identification of the other member states, and finally mandatory mutual recognition of eIDs will apply from 2018.[97]

Essentially the eIDAS Regulation will enable secure electronic interactions between businesses, citizens and public authorities intended to increase e-commerce in the EU as well as variety of private online services.

6. Data Protection Reform

The current legal framework on data protection, including Directive 95/46/EC,[98] and ePrivacy Directive 2009/136/EC[99] remains sound as far as objectives are concerned.[100] Yet, the complexity

93 *See, e.g.,* Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. COM(2012) 238 final. European Commission, 3 (2012)

94 Id.

95 Trust services, Digital Agenda for Europe, European Commission. Available: http://ec.europa.eu/digital-agenda/en/trust-services#Article Accessed: 26.11.2014.

96 Eleventh Report of Session 2012-2013, European Scrutiny Committee, House of Commons, at 31, 32 (2012)

97 Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ 2014 L257/73 [eIDAS regulation]

98 Data Protection Directive (1995), supra note 55

99 ePrivacy 2009 amendment, supra note 75

100 Art. 16(1) of Treaty on the Functioning of the European Union (TFEU) establishes the principle of Lisbon Treaty that everyone has the right to the protection of personal data concerning him or her, and Art. 8 of the Charter of Fundamental Rights of the EU enshrines protection of personal data as a fundamental right.

remains a major problem, hence in 2012 the Commission proposed a major reform of the EU legal framework on the personal data protection for more coherence.[101]

The data protection reform package consists of two proposals, a General Data Protection Regulation covering the personal data processing and free movement in the European Union,[102] and a Directive on processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, and free movement of data.[103]

The goal of proposed General Data Protection Regulation is to further strengthen the individual rights such as right of data portability addressing the central role of personal data protection and control to respond to the challenges of globalisation and new technologies such as cloud computing.[104] Reform package would provide means to keep up with the changes in emerging technologies in ICT covering *inter alia* data processed on the internet, social networks, online shopping and e-banking, hospital registers and personal data held for research purposes.

The right to be forgotten was articulated in the Draft Proposal for a General Data Protection Regulation in 2012, although the idea existed already in Directive 95/46/EC. It was seen that the 'right to be forgotten' further established by Court of Justice in the Judgment of 13 May 2014 in *Case 131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* [2014],[105] needs to be clarified for the digital age.[106] In what form it will be in the legislation, remains unclear. As an example, right to be forgotten in

---

101 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Safeguarding Privacy in a Connected World a European Data Protection Framework for the 21st century (2012)

102 Proposal for Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2012) [Proposal for Data Protection Regulation (2012)]

103 Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data COM(2012) 10 final (2012) [Proposal for Data Protection Directive (2012)]

104 Proposal for Data Protection Regulation (2012), supra note 102

105 *Case 131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* [2014] EU:C:2014:317 [Case Google Spain 2014]

106 *See, e.g.* European Commission, *Factsheet on the "Right to be Forgotten" Ruling (C-131/12)* Available: *http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf* Accessed: 16.11.2014

the Article 17 of Commission Proposal for General Data Protection Regulation was in the form 'Right to be forgotten and erasure' whereas in the European Parliament vote it was reformulated into 'right to erasure'.[107]

As European Data Protection Supervisor (EDPS) formulates, EU rules on data protection need to be reformed urgently in order to provide more consistency[108] and coherence[109] in data protection across the EU, thus creating a level playing field, both for online and traditional market players.[110]

7. Counter Terrorism and Invalidated Data Retention Directive

The Data Retention Directive compelled member states to ensure that telecommunications service providers and operators retain and store clients' personal data "in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime".[111] The categories of data that was to be retained for a period between six months and two years were *inter alia* data necessary to trace and identify the source of a communication; data necessary to identify the destination of a communication; data necessary to identify the date, time and duration of a communication; and data necessary to identify the location of mobile communication equipment.[112]

Directive was a legal response in fight against terrorism, but does not limit data retention to combating terrorism. It was adopted in the aftermath of the terrorist attacks in Madrid in 2004

---

107 *See* European Commission Memo 14/186 *Progress on EU data protection reform now irreversible following European Parliament vote* (2014) Available: http://europa.eu/rapid/press-release_MEMO-14-186_fi.htm Accessed: 16.11.2014

108 Effective protection of citizens fundamental rights to privacy and data protection can only be delivered if the applicable legal framework is coherent i.e. covers the broadest possible range of data processing entities and activities

109 Applied in a manner as uniform as possible among all 28 member states.

110 *See* EDPS letter to the Council of Ministers regarding progress on the data protection reform package on 14 February 2014, *Progress on the data protection reform package* (2014) Available: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2014/14-02-14_letter_Council_reform_package_EN.pdf Accessed: 16.12.2014

111 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 2006 L105/54 [Data Retention Directive 2006]

112 Id.

and in London in 2005 to make the fight against terrorism more effective by e.g. harmonizing the definition of terrorist offences,[113] although the transposition of the Directive was incomplete in several member states.[114]

What is illustrating is that already the proposal for Data Retention Directive was seen to possibly infringe the Article 8 ECHR.[115] As Hustinx notes, "retaining communication and location data of all persons in the EU, whenever they use the telephone or the internet, constitutes a huge interference with the right to privacy of all citizens. The Directive is without doubt the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects."[116]

The Data Retention Directive was invalidated in *joined Cases 293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and *594/12 Kärntner Landesregierung and Others,* [2014] EU:C:2014:238. The Court of Justice took the view that "by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data" and "by adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality".[117]

---

113 EU framework decision is designed to make the fight against terrorism at EU level more effective. *See* Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism OJ L164/3, and its amending Act Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism OJ 2008 L330/21

114 For political controversies on systematic retention of communications traffic data, difficulties for operatiors and uneven playing field, *see* I. Walden, Telecommunications Law and Regulation (2012)

115 *See, e.g.,* Article 29 Data Protection Working Party. Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism, 3, 6, 7 (2004) Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp99_en.pdf Accessed: 26.11.2014

116 P. Hustinx, *The moment of truth for the Data Retention Directive,* Conference 'Taking on the Data Retention Directive',1 (2010) Available: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf Accessed: 15.12.2014

117 Court of Justice of the European Union, *The Court of Justice declares the Data Retention Directive to be invalid* (2014) Available: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf Accessed: 16.12.2014

III. Other Sources of Law

1. CJEU Case-Law

Court of Justice of the European Union (CJEU), established in 1952 has as its main functions, to review the legality of instruments of the European institutions and of governments; give rulings, at the request of a national courts and tribunals on the interpretation or the validity of provisions in European Union law i.e. preliminary rulings; and to ensure that the member states comply with obligations under the Treaties.[118]

Court settles legal disputes between EU governments and EU institutions. Individuals and legal entities can also bring cases before the Court in certain cases prescribed by treaties if they feel their rights have been infringed by an EU government or institution.[119]

In the *Case 101/01, Bodil Lindqvist v Åklagarkammaren i Jönköping,* [2003] EU:C:2003:596, publishing of *inter alia* names and phone-numbers on personal website is considered processing of personal data. Furthermore, the reference to the injured foot was considered as prohibited processing of sensitive personal data.

Right to be forgotten was considered in *Case 131/12 Google Spain* 2014[120] where in its Judgment of 13 May 2014 the Court held that the operator of a search engine is obliged to remove from the list of results displayed, for search by individuals name, published by third parties, information relating to that person. In addition under Article 7 – Respect for private and family life and Article 8 – Protection of personal data of the Charter of Fundamental Rights of the European Union[121] data subject may request that the information in question no longer be made available to the general public. This is possibly overriding not only the economic interest of the operator of

---

118 Court of Justice of the European Union, General presentation (2014) Available: http://curia.europa.eu/jcms/jcms/Jo2_6999/ Accessed: 9.12.2014

119 Article 265 of the Treaty on the Functioning of the EU provides "Any natural or legal person may, under the conditions laid down in the preceding paragraphs, complain to the Court that an institution, body, office or agency of the Union has failed to address to that person any act other than a recommendation or an opinion". For example The Treaty requires Parliament, the Council and the Commission to make certain decisions under certain circumstances, and if they fail to do so in addition to preferential plaintiffs i.e. member states and EU institutions, also individuals may be able under certain conditions to bring proceedings before the Court of Justice.

120 Case Google Spain 2014, supra note 105

121 The Charter of Fundamental Rights of the European Union, supra note 52

the search engine but also the interest of the general public in having access to that information through search engine.[122]

The invalidation of data retention directive in *joined Cases 293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and *594/12 Kärntner Landesregierung and Others,* [2014] EU:C:2014:238 means that ePrivacy Directive 2002/58/EC[123] prohibiting data retention, except where it is "necessary, appropriate and proportionate" for national security purposes applies after the judgment. This is because the ePrivacy Directive[124] was amended by the Data Retention Directive[125] to remove prohibitions on data retention. European Commission is now required to enforce the general prohibition on data retention and member states who have already implemented the invalidated Data Retention Directive[126] in a national level, have to consider the options and are in a rather unique position to invalidate, amend or interpret the national law in a new way, since it is not in compliance with a European Union law.

Judgment of 19 December 2013 in *Case 202/12 Innoweb BV v Wegener ICT Media BV and Wegener Mediaventions BV,* [2013] EU:C:2013:850 concerned *sui generis* right of the database maker. Court held that the essential features of a dedicated meta-search engine clearly distinguish it from a general search engine like Google or Yahoo, and ruled that operator who makes available on the internet dedicated meta-search engine infringes the rights of database maker under Article 7(1) of Directive 96/9/EC[127], by re-utilizising the whole or substantial part of the content of the database.[128] Although meta-search engines were distinguished from traditional search engines, they may use similar search technology. Hence distinction between meta-search and general search engines can be seen artificial.[129] The purpose of a meta-search engine is to

122 For right to receive and impart information without the interference by public authority, *see* Art 11 – Freedom of expression and information of The Charter of Fundamental Rights of the European Union, supra note 52

123 ePrivacy Directive 2002, supra note 69

124 Id.

125 Data Retention Directive 2006, supra note 111

126 Id.

127 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases OJ 1996 L77/20

128 *Case 202/12*, *Innoweb v Wegener* [2013] paras. 47, 49, 50

129 P. Virtanen, *Innoweb v Wegener: CJEU, sui generis database right and making available to the public – The war against the machines*, 5 EJLT Commentaries (2014) [*Sui generis* database right]

provide more informative and user-friendly results.

2. ECtHR Case-Law

To ensure that the contracting states respect their obligations under the European Convention on Human Rights (ECHR), the European Court of Human Rights (ECtHR), was set up in 1959. Throughout its jurisprudence the ECtHR has considered many cases regarding privacy.

Interception of communication is considered inter alia in *Malone v. the United Kingdom,* ECHR (1984), Series A, No. 82 where it was found that Article 8 of the European Convention on Human Rights (ECHR) may be engaged where information is gathered for a legitimate purpose, but disclosed to a third party for other reason than original. As Judge Pettiti noted on his consenting opinion, "[i]t is known that, as far as data banks are concerned, the processing of 'neutral data' may be as revealing as the processing of sensitive data."[130] This indicates that previously it was decisive whether the infromation was sensitive, whereas in modern broader approach personal data and systematic collection are decisive.

Further, the Court has clarified that Article 8 of the ECHR[131] not only obliged states to refrain from any actions which might violate rights but states are also under positive obligations to actively secure effective respect for private and family life in ECHR, *I. v. Finland*. ECHR (2008) Application No. 20511/03.

In *S. and Marper v. the United Kingdom* ECHR (2008) Application No(s). 30562/04 and 30566/04[132] it was held that retention of DNA samples, fingerprints and cellular samples of individuals arrested but who were later acquitted or charges dropped is a violation of the right to privacy conferred in Article 8 ECHR.[133] Court pointed out that not only the use is a violation, but also the mere collection constitute a disproportionate interference with the right to respect for private life and the indefinite retention of fingerprint and DNA material of any person of any age suspected of any recordable offence failed to strike balance between the competing public and

130Concurring opinion of Judge Pettiti (translation) *in Malone v. the United Kingdom,* ECHR.
131Art. 8 of the European Convention on Human Rights
132Published in Reports of Judgments and Decisions 2008
133Art. 8 of the European Convention on Human Rights

private interests.[134] United Kingdom is know to be the pioneer in using modern technologies in fight against crime and in forensics. Hence they can be seen to bear special responsibilities in assessing the limits of the interference with private life.[135]

The balance between right to privacy and the freedom of expression under the European Convention on Human Rights is considered in *Von Hannover v. Germany (no. 2*) ECHR (2012) Application No(s). 40660/08 and 60641/08 [136] in which the background for the case was pictures of Caroline, Princess of Hanover, and her husband published by a magazine, which served as an evidence that the princess was on holiday whilst her father was seriously ill. Princess Caroline alleged the pictures were violating her right to privacy and that national courts failed to protect her on the ground that she was a figure of contemporary society '*par excellence*'. Court held that there has been no violation of Article 8 ECHR[137] by observing that the national courts balanced the right of the publishing companies to freedom of expression against the right of the applicants to respect for their private life. Court considered that it contributed to a debate of general interest,[138] and circumstances were considered in which the photos had been taken.[139]

The balance between right to privacy and the freedom of expression was considered also in *Axel Springer AG v. Germany* ECHR (2012) Application No. 39954/08, where the publisher of the newspaper brought a complaint, alleging an undue restriction of the freedom of expression in a case where an article was written on an actor who had been arrested for possession of drugs at the Munich Oktoberfest. The actor successfully applied for an injunction in Germany.

Cases *Von Hannover v. Germany (no. 2*) and *Axel Springer AG v. Germany* ECtHR sets up criteria for the balancing exercise[140] where the outcome should be the same regardless of whether the claims are on a violation of privacy – in *Von Hannover*, or restriction of the freedom of expression – in *Springer.*

134 Paras. 60, 110 and 125 of the Judgment *in S. and Marper v. the United Kingdom* ECHR (2008) Application No(s). 30562/04 and 30566/04

135 Id. para. 112

136 Published in Reports of Judgments and Decisions 2012

137 Art. 8 of the European Convention on Human Rights

138 Para.109 of the Judgment *in Von Hannover v. Germany (no. 2*) ECHR (2012) Application No(s). 40660/08 and 60641/08

139 Para.113 of the Judgment *in Von Hannover v. Germany (no. 2*) ECHR (2012) Application No(s). 40660/08 and 60641/08

140 Balancing exercise between Art. 8 – Right to respect for private and family life and Art. 10 – Freedom of expression of the European Convention on Human Rights

In *Konovalova v. Russia* ECHR (2014) Application No. 37873/04*,* the ECtHR considered whether allowing medical students to observe a childbirth without the mother's explicit consent violated her right to privacy, and more specifically with the requirement of lawfulness of Article 8(2) ECHR.[141] The Court reiterated that under its case-law, the concept of 'private life' is a broad term not susceptible to exhaustive definition including among other things physical and moral integrity.[142] It was seen interfering her privacy rights within the meaning of Article 8 ECHR and was not in accordance with the law in the meaning of the Article 8(2).[143]

IV. Concluding Remarks

Pre-internet context and subsequent gradual development is visible in the European regulatory framework creating a very encompassing but relatively complex framework for ePrivacy in ICT. Also specific strategies such as EU counter-terrorism strategy created confusion among member states although the objective was to make fight against terrorism more effective by e.g. harmonising the definition of terrorist offences.

Conclusion can be made that quest for equilibrium between fundamental rights such as ePrivacy rights and the protection of personal data;[144] economic interests; as well as universal threats such as terrorism limiting the right to privacy has been challenging in European regulation. As a most recent example on these challenges, the invalidation of the Data Retention Directive 2002/58[145] by CJEU.[146]

141 Art. 8 of the European Convention on Human Rights
142 Para. 39 of the Judgment *in Konovalova v. Russia* ECHR (2014) Application No. 37873/04
143 Paras. 40, 41 of the Judgment on the interference and paras. 42, 48 and 49 on the requirement of lawfulness *in Konovalova v. Russia* ECHR (2014) Application No. 37873/04
144 Privacy and the protection of personal data are closely linked, but they should not be considered to be identical, *see, e.g.,* Privacy and data protection in the CJEU and ECtHR, supra note 12
145 Data Retention Directive 2006, supra note 111
146 Judgment of The Court *in joined cases C-293/12, Digital Rights Ireland Ltd v Minister for Communications and others* and *C-594/12, Kärntner Landesregierung and Others* [2014]

C. Emerging ePrivacy Implications – Patents as a Source

This chapter is divided into three parts. In the first part general considerations regarding patents as a source of data for the research are made. In the second part 'Selecting Patents' emerging technologies are identified by analyzing different stages of patent filing process, applications and granted patents. Further, by combining information on these two stages of patent application process it is possible to calculate the success rate of a patent applications i.e. potential of emerging technologies to be utilized having actual implications on ePrivacy and relevant for analyzing the European regulatory framework.[147] The most relevant patent classes were identified by WIPO PATENTSCOPE and EPO PATSTAT.[148] Patent documentation is selected for the qualitative analysis by using Global Patent Index (GPI) search.[149] In the third part 'Analysis on Patent Documentation' the patent documentation of selected ICT patents is studied qualitatively for the purpose of identifying ePrivacy related implications.

I. General Considerations

1. ICT Patent Classes

The OECD suggestion of ICT related classes where IPC codes are assigned to ICT patents was used.[150] Although the terminology used by OECD, WIPO and EPO may slightly differ, the patent classes used in research follows the taxonomy of International Patent Classification Standards (IPC), hence all presented information is comparable regardless of whether it is gathered from

147 Industrial applicability in European Patent Regime suggest that technology for which protection is provided should be used to create business around inventive technological solution to an existing problem.

148 WIPO PATENTSCOPE online search in http://www.wipo.int/patentscope/en/ , and EPO PATSTAT in http://www.epo.org/searching/subscription/patstat-online.html. The PATENTSCOPE database includes published PCT international applications and bibliographic data and documents contained in the files of PCT international applications from national and regional patent offices. The PATSTAT database includes data from EPO master bibliographic database DOCDB. The database is updated twice a year in April and October. Current database is updated in October 2014.

149 GPI is a subscription service with advanced search options, but the search can be conducted also with combining publicly available services by EPO such as Espacenet and PATSTAT.

150 OECD Guide to Measuring the Information Society 2011, 64-66 (2011) [OECD Guide 2011]

WIPO, OECD or EPO database.[151] (See Appendix 1)

For emerging technologies, a category or class might not yet be incorporated in the patent classification systems, which makes it difficult to identify patents related to these emerging technologies considering e.g. the future research validation. However, each patent grant is assigned to at least one IPC class in order to determine the nature of the patent.[152] This means that if emerging technology does not fit into existing categories, it can be assumed that numerous classes are assigned.[153]

2. Limitations

Patent data is not the only implication of emerging technologies, but technology that gets a patent granted has implications on the technology field and on regulatory framework. When studying regulatory framework for ePrivacy in the European Union level, the source of data needs to be accessible, reliable and well structured. Considering the European regulatory framework, the patents granted at the EPO may not be of specifically European relevancy, although it is an assumption that if patent applications are filed at the EPO the data processor intends to operate on European market in addition to other possible markets. It was seen beneficial to further define that only patents in which the applicant is from the EU 28 countries, were used.

Patents do represent inventions, but only potentially innovation. Invention is the product of, bright mind, usually technological, and innovation describes the utilization and exploitation of such idea. Thus, statistical information on ICT patents is better to be understood as an input than an output indicator, but it can serve as an indicator.[154]

One aspect of method used to find relevant classes for emerging technologies, the amount of patents in classes, may be affected by the fact that certain classes may be seen to attract most of

151 The advantage of using the IPC classification system is that it is used by a large number of patent offices, which makes it possible to derive comparable ICT-related patent statistics.
152 Patent can be assigned also to more than one IPC if the patent finds application in various domains.
153 This is due to the fact that if patent does not fit into any particular class, it is assumed to cover several classes rather than alternatively left outside the classification and this is hardly the case in any situation.
154 M. Rogers, The Definition and Measurement of Innovation, 11 (1998)

the patents in certain technological domain, but this does not however mean that these technologies are less relevant, but quite contrary. It is important to understand that granted patent can have several sub-classes, not only one. Thus, the selection of the most relevant sub-classes made in quantitative analysis introduced classification to increase the quality of the processing and analyzing the data but do not exclude potential patents.[155]

II. Selecting Patents

1. Relevant Patent Classes

Query on WIPO Patentscope for 'internet' provides that the main IPC is G06F with 455 540 results. Term was in 2004 used 69 685 times, whereas in 2013 100 804 times implicating significant growth in internet related patents. The growth rate from 2004 to 2013 was 44.7% and from 2012 to 2013 11,2%.

Query 'cloud AND computing' indicates that the main IPC sub-classes for cloud computing are G06F and H04L. Terms were used together in patent documents 2408 times in 2004, and 22 088 times in 2013. The growth rate from 2004 to 2013 was 817%, and from 2012 to 2013 51.5%.

Main IPC for query "mobile AND device' was G06F with 224 711 results, and terms were used together 58 669 times in 2004 and 118 746 times in 2013. The growth rate from 2004 to 2013 was 102.4%, and from 2012 to 2013 13.6%.

The most potential emerging technologies based on growth rate analysis are in sub-classes *G06F Electric Digital Data Processing* and *H04L Transmission of Digital Information, e.g. Telegraphic Communication.* G06F is in included in 'Computers, office machinery' category, and H04L in 'Telecommunications' category.

For mainly triangulation purposes, the search was conducted in addition to granted patents, also on EPO PATSTAT patent application database EPAB 2014/45. The most significant IPC sub-classes were also G06F and H04L.

155If emerging technology does not fit into existing taxonomy, several sub-classes are assigned.

2. Relevant Patents

To select the specific patents granted from most relevant classes identified, EPO Global Patent Index (GPI) service was used.[156] The search was limited to cover the identified IPC classes H04L and G06F.

With Boolean query (IPC = H04L AND IPC = G06F AND TEXT = privacy AND CYE = YES) ANDNOT TEXT = medical +1w device. Query resulted in 52 documents.

Kind code B1 on patents indicate that patent protection is granted without amendments, oppositions or limitation procedures.[157] Due to this fact 'PUK = B1' was added to the boolean query:

(PUK = B1 AND IPC = H04L AND IPC = G06F AND TEXT = privacy AND CYE = YES) ANDNOT TEXT = medical +1w device. Query resulted in 25 granted patents.

The documentation of these 25 patents were reviewed and selection was made based on the subjective analysis on their relevancy in finding answers to the research questions.

Following patents were selected for qualitative analysis:

1. EP2613499

'A communication system for tagging communication artefact'. Publication date 19.3.2014, European Patent Bulletin 2014/12. IPC classification: H04L 12/58, H04L 29/08, G06F 17/30 and G06Q. Applicant / Proprietor: Alcatel Lucent.

2. EP2389641

"EINRICHTUNG ZUR GENERIERUNG EINES VIRTUELLEN NETZGÄNGERS' (SYSTEM TO GENERATE A VIRTUAL WEB SURFER). Publication date: 12.3.2014, European Patent Bulletin 2014/11. IPC classification: G06F 21/41, G06F 21/62, G06F 21/77 and H04L 29/06. Applicant / Proprietor: Uniscon universal identity control GmbH.

---

156 Global Patent Index (GPI) is a non-public EPO patent information service for experts and the access is restricted to subscribers. *See* https://data.epo.org/expert-services/start.html Accessed: 15.11.2014

157 *See* EPO kind code concordance list. Available: http://documents.epo.org/projects/babylon/rawdata.nsf/0/8DC80ADFE1BADAF1C1257B1A0048C057/$File/Concordance_20140723.xlsx Accessed: 15.11.2014.

3. EP2513799

'A METHOD, SERVER AND COMPUTER PROGRAM FOR CACHING'. Publication date: 12.3.2014, European Patent Bulletin 2014/11. IPC classification: G06F 12/12,G06F 17/30 and H04L 29/08. Applicant / Proprietor: Telefonaktiebolaget L M Ericsson.

3. Concluding Remarks

With selected method it was possible to accurately identify firstly relevant patent sub-classes, and secondly specific patents for qualitative analysis.

Yet, patent-based indicators in statistical analysis should never be considered as a proxy on their own, since they do not explain external effects such as competition, regulatory framework or other relevant aspects. Hence the subjective selection from classified patent documentation was essential to reach the future-oriented aspect of emerging technologies.

III. Analysis on Patent Documentation

The information disclosed in patent documentation was reviewed and main findings are presented. Information is used in chapter 'D. Discussions' to make conclusions on the implications of these emerging technologies and consequently the European regulatory framework is analyzed.

1. EP2613499 – A Communication System for Tagging Communication Artefact

The invention relates to communication technologies and the managing of pertinent information relating to corporate projects.

Description part of the patent documentation identified the problem relating to the communication and sharing of information. It was identified that information about a project is not kept in public documents or web pages, but mainly discussed in mail threads, instant

messaging sessions, phone talks, teleconferences, or other private by nature media. The purpose of the patented technology is to aggregate and store the information and to make the information accessible to all the stakeholders. Invention relates to a particular method to gather information and share the knowledge to the stakeholders without the need of manual processing of the information such is the case in prior art systems. [158]

The invention is a communication system, such as a corporate communication system comprising a tagging means for tagging a communication artefact with at least one thematic contextual tag, and a communication artefact storage for storing communication artefacts automatically.

A communication artefact according to claim two, can be but is not limited to *inter alia* an instant messaging session, phone call obtained by automatic speech recognition tool,video conference call or any other file containing information that is wanted to communicate to a stakeholder that can be for example a third person who joins a project afterwards.

The tagging of a communication artefact triggers the storage means to automatically store the communication artefact or a copy of it in a storage. The thematic tagging first provides a way to sort the communication artefact e.g. to ease a future retrieval, and second it automatically stores the communication artefact in a public repository, i.e. it publishes communication artefact that was private before, so that it can be publicly accessed.

The tags can also be organized and used to publish and publicise communication artefacts that may be otherwise private by nature, such as mails or instant messages. However, in the context of a corporate system, it can be considered that even private by nature communication artefacts are means dedicated to work and sensitive data can be exposed creating situation where private information is made public that should not have been processed.

User can keep a communication artefact private. This can be done implicitly by not tagging said communication artefact or by using at least one dedicated 'private' tag, or equivalent, that forbids the publication of so tagged communication artefact. In order to further protect privacy, according to one feature, the tagging means may only authorise an owner of a communication artefact to tag its own communication artefact. Only the owner of a communication artefact is

158 See patent EP2613499, especially paras.1-5.

allowed to determine if a communication artefact can be published.

As the first claim explains that tag is a thematic contextual tag. One of the most important aspect from the privacy perspective relates to the fact that the tag is a thematic contextual tag. It provides new possibilities to software-read data. This means in a more simplistic terms that the information on a communication artefact such as email or internet page can be 'understood' by software. This creates the possibility to make connections but also process information in thematic context level. This leads to the fact that business related information such as trade secrets and intangible knowledge is turned into form that can be further processed, but also personal data included in communication artefacts is processed.

By annotating communication artefacts with semantic meta-data,[159] software can automatically understand what the documents include by combining various tags i.e. meta-data, unlike traditional statistical or concurrence analysis which explaining only relationships but does not understand the content. This development can be understood as an implication of semantics powered web.

2. EP2389641 - Einrichtung zur Generierung eines Virtuellen Netzgängers

The technical domain is a communication system and more specifically a device for generating a virtual web surfer i.e. virtual network user that can be used to gain a certain level of privacy by the means of a pseudonym identity.[160] Invention provides possibility for a physical person or a legal entity to gain access to the internet and engage services by online service providers whilst maintaining certain level of anonymity and privacy.

As explained in an abstract, the virtual network user is defined by a freely specifiable combination of attributes. The transformation system can be activated by the network access device of the user such as a personal computer or a tablet, which in turn facilitates the generation

159 Semantic meta-data describe contextually relevant information about content. For more information on semantic meta-data, s*ee, e.g.,* A. Sheth & K. Thirunarayan, Semantics Empowered Web 3.0 Managing Enterprise, Social, Sensor, and Cloud-based Data and Services for Advanced Applications (2013)

160 The pseudonym refers to a virtual identity for the purpose of concealing the real identity of the natural or legal person in the virtual world for particular purpose. It does not make the user invisible rather creates virtual identity based on given attributes.

of the data flows that implement the virtual network user. This 'avatar' or pseudonym can in addition be saved with the temporal sequence of the data flow in a storage device of the transformation system for possible future use.

The object of the invention is to design a method and a device that, with due respect for the confidentiality of the identity of the natural or legal person nevertheless in case of urgent need, e.g. for the purpose of preventing a crime an adequate accessibility of state authority is given to the information of the user of the pseudonym.[161]

The invention limits the anonymity of the user, being reasonable and balanced to the objects, which serve a good balance of individual and social interests. For example additional assurance is provided that only data which is necessary for the investigation of an offense or its prevention is provided for public authority in a predetermined frame which is in accordance with the law e.g. excluding access to highly personal data that is not related with a crime.

Several claims are presented, for example fingerprint or other biometric sensor for multiple network surfer roles, encryption of the identity relevant traffic data that can be encrypted with different keys, high level of security against unauthorized access to personal data and authentication module for the detection of a minimum age, gender or nationality.

In the drawings of the patent documentation, additional functionality can be identified. The device is designed so that virtual web surfer will be generated according to the user specified attributes whether very similar to real identity or clearly imaginary avatar, however, before it can be active in the network and access is authorized for example proof of user's legal capacity must be given. It is also possible to restrict the use e.g. user have to agree that the state's authority, under the rule of law, is granted access to the information and possibility for tracking.

Also the possibility of access for third parties is included for implementation of new services. For example a logistics company can have access to the information necessary for the service such as authentic address. If considered further it is possible to give the delivery address which can be different from the address of the user and only relevant for specific delivery.

In addition, invention contributes to the data protection by conveying the function of mixing

161 According to the invention this objective is achieved by the method explained in claim 1 and by the device in claim 7.

nodes in which the collected data streams repetitions are deleted, recoded and re-sorted so that the origin of the message is obscured in the outcome.

Invention provides possibility to demonstrate that contracting parties have expressed consent and are identified. By this, it is possible to make contracts and identify user to extent necessary for the purpose. Although, it can be assumed the concept of digital signature and possibility to make legally binding contracts by signing contract with fingerprint reader or other biometric data reader which is used by plug-in device must be considered in regard to national law and for the cross-border e-commerce harmonized legal framework needs to be in place.

As a final note, it seems to be that the invention was made taking into account the Data Retention Directive 2006/24/ EC and as a practical implication of legal uncertainty, due to fact that directive is invalid some features may not be fully compatible with the current EU regulation such as Directive 95/45/EC or General Data Protection Directive in the future.

3. EP2513799- A Method, Server and Computer Program for Caching

The invention relates generally to caching and more particularly to improving caching accuracy.

As explained in the description of patent documentation, caching media is a technique for improving access times and optimizing bandwidth usage in telecommunication and enterprise networks. A cache uses a block of memory to temporarily store a copy of some data that is likely to be needed in the future.

When cache clients such as computers or mobile terminals try to access data, they check the cache first. If the necessary data is available in the cache, then cached copy is used. If the data is not found in the cache then it is downloaded from the original source and also stored for later access.

When new data is stored in a cache, often some previously cached data has to be removed in order to free up storage capacity. The strategies that determine what data should be removed are called caching algorithms or caching replacement algorithms.

According to claim one, a method for caching comprising the steps of: determining in a caching server of a telecommunication network a user profile to analyze; obtaining in the caching server

a group of user profiles; obtaining correlation measurements for each user profile in the group of user profiles in relation to the user profile to analyze; and finally calculating a content caching priority for at least one piece of content of a content history associated with the group of user profiles, taking the correlation measurement into account.

By considering correlation between users, improved accuracy of the caching will be achieved. This will result in fewer cache misses and more cache hits, which improves the performance of the caching using the method. The step of obtaining correlation measurements may comprise obtaining correlation measurements from a central correlation measurement provider server in the telecommunications network, and can be distributed regularly or on demand.

By calculating the correlation measurement only when requested, i.e. on demand, the most recent data can be considered, yielding a more accurate correlation measurement. This can be performed centrally or in a node at a lower level of the network hierarchy, that is a node which is closer to the clients.

The correlation measurements may also be calculated using correlation data provided by a third party through an external application programming interface. Third parties can have more data on relationships between users in the system, which thus gives a more accurate correlation measurement and thereby better caching. The step of obtaining a group of user profiles may comprise obtaining a group of all user profiles currently associated with the caching server. In other words, the relations to all users associated with the caching server are processed in order not to leave any potential relation out between the analyzed user and users under the caching server.

The method may be started in response to the user profile becoming associated with the caching server. For example, this can occur in a mobile network when the user of the user profile moves into an area of responsibility of the caching server. Also the caching priority can be set. This allows differentiation in caching for various users. For example a viewed video can be more important that the accessed web page.

It is mentioned in the invention that the data storage in the caching servers of the technology is temporary, hence the privacy of the user is not at risk. For longer periods, the user history data base stores for longer intervals only aggregate information related to general characteristics of

the data that was accessed by a particular user. Regardless of this it can be assumed that the cache provides possibility to the processing the data e.g. store the circumstances when a piece of data was downloaded *inter alia* the downloading user's location, time of day and content accessed previously hence obtain even sensitive personal data such as ethnic origin, religious beliefs or sexual orientation.

4. Concluding Remarks

The patent EP2613499 explains technology that creates meta data by tagging communication artefact which can be understood by software agents. This means that the information can be thematically tagged for sharing the information. Tagging does also provide the possibility to process the data by means of Big Data, and if privacy is not protected by technological means such as cryptography and relevant or absorbant existing law not in place, tags providing further information can leak and cause serious harm for privacy.

The patent EP2513799 explains that the third party can be a server with access to some form of content history of the user. For example, a video content website can have information that 80 percent of users that request content A also requests content B. In a situation where content A is requested, it would be beneficial to pre-fetch content B, or if elaborated idea further to advertise content B to change the consuming behaviour of the user. Furthermore, online shopping platforms can register preferences for different types of content for each user, along with relationships between users. Inferring some of this information from unencrypted traffic within the network would provide to be very valuable for businesses or cyber criminals.

It is sufficient to note that considering the features of the invention in patent EP2389641, criminal use of the device is possible by taking action under pseudonym although the tracing of the data track can be done by public authority with its features.[162] However, the biggest challenge in online world is due to its distinctive features such as limitations of territoriality of law and challenges in identification of, not necessarily the IP address and other revealing information, but of the person. Finally, in current European regulatory framework, 'virtual net surfer' can be

162 The Directive 2006/24/EC on data retention in the telecommunications was taken into account in this patent.

considered as a Privacy Enhancing Technology (PET) providing identity management solution that manage the individual's online identity and empower the private person as well as businesses to actively protect their privacy.[163]

IV. General Conclusions of Patent Research

To give an answer to the research question, “Based on research on ICT patents, what are the most significant implications emerging technologies in ICT have on ePrivacy?”, the implications emerging technologies have on regulatory framework, can be seen as two-fold. Firstly, new privacy concerns related to the storing and later retrieval of the user data, and the emergence of Big Data and the new possibilities to use data, such as processing the meta-data with software. Secondly, in addition to threats, ICT may actually provide suitable and efficient solutions to privacy problems.

The identified implications of emerging technologies in ICT do indicate that ePrivacy will be a focal point in the European regulatory framework and increasingly important to consider when the methods of Big Data are spreading, the storing of data (processing) becomes a very important factor, and cryptography and its applications such as digital signature and encryption becomes more important as a necessary enabler for many other technologies and concepts such as eGovernance.

Research question “Are patents an adequate and suitable source of information for analyzing privacy issues regarding ICT in the future from the legal perspective?” should be answered by considering it from several aspects. Goals for information gathering from patent data was achieved in terms of availability and quality. Although, the 'EPO GPI advanced tool for searching patent data' was used, the non-subscription and free to use search tools e.g. Espacenet and PATSTAT provide tools for everybody interested to study most recent developments and,

163 PETs are technologies that may inter alia provide multiple virtual identities i.e. to anonymize communication and manage personal data. See for more on privacy-enhancing identity management and how it can be realized in software, R. Leenes, J. Schallaböck & M. Hansen, PRIME white paper, Privacy and Identity Management for Europe (2008) Available: https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf Accessed: 27.11.2014

historical patterns in variety of technological fields.[164]

It must be noted that patents as a source of data for legal research seems to be very novel idea especially in Europe since similar legal academic research did not exist and information from European perspective and on European patents was challenging to find.[165] This fact lead into the conclusion that the data was first to be collected specifically for the thesis in order to analyze current regulatory framework and make well-founded conclusions and recommendations. For this purpose patents were among only few possible sources.

Although conclusions are inherently subjective, the value in conducting research on patents lies in the fact that conclusions and recommendations are not based on repetition of existing studies, but on unique information gathered solely for the purpose of this thesis, yet analyzed in the framework of legal research being complementary to traditional sources of legal information.

164 GPI was used instead of Espacenet due to the possibility to combine queries saved in the query history, use boolean operators, and to download results in XML format.

165 Example on how versatile patents are as a source of information, *see* A. Barney & A. Jonathan, *Study of Patent Mortality Rates: Using Statistical Survival Analysis to Rate and Value Patent Assets*, 30 AIPLA Quarterly Journal 319 (2002)

D. Discussions

In this chapter, the European regulatory framework for ICT is discussed based on identified privacy implications. This chapter identifies possible weaknesses and problems in current regulatory framework in ePrivacy related issues.

First part 'I. Past Ideology' considers in theoretical level the interplay between law and technology on how the privacy and ePrivacy differs. The aim is to position the ePrivacy related issues into the historical perspective and understand the continuously shaping concept of privacy. It is also captured how privacy concerns reflect the society through case-law.

Second part 'II. Present Law' analyzes privacy issues in ICT from legal perspective and with legal research tools. The present regulatory context is discussed based on implications found from patent research. In this chapter the emphasis is not on the constraints law imposes to emerging technologies, but rather how the legal landscape appears for new emerging technologies from the ePrivacy perspective.

I. Past Ideology

1. Reflections of Society

Already in 1890 Warren and Brandeis referred to the next step which must be taken for the protection of the person.[166] The earliest definition of privacy in English law was given by Judge Thomas Cooley who defined privacy as a negative right, the right to be left alone: “The right of privacy, conceding it to exist, is a purely personal one, that is a right of each individual to be let alone, or not to be dragged into publicity.”[167] As Adrian has pointed out, the right to privacy has been seen primarily as a human or social right arising from the nature of the relationship between the individual and society deriving from the thinkers such as Hobbes and Locke.[168]

166 The Right to Privacy, supra note
167 Classification of legal rights, supra note 4
168 A. Adrian, *Has a Digital Civil Society Evolved Enough to Protect Privacy,* 37 Alt. LJ 183, at 184 (2012)

Considering the more recent developments in society such as the convergence of the physical and virtual world, and the growing role of technology, it can be argued that the normative approach on understanding privacy and the clear-cut distinction between public and private spheres is in *cul-de-sac* and contextual approach on privacy is gradually superceding. In addition the distinction between informational and physical privacy is becoming more and more insubstantial.[169] This development can be seen in lively discussions in jurisprudence reflecting the re-conceptualization of privacy understanding that every sophisticated legal approach on data protection should incorporate insights and concepts from other disciplines.[170]

To understand how privacy online i.e. ePrivacy is different from privacy, the conceptualization of privacy in digital world by Nissenbaum captures one of the most essential features of ePrivacy defining it not only in terms of right to control own information, but extending it to expected flows of personal information emphasising that the right to privacy is not a right to secrecy, nor a right to control information, but a right to appropriate flow of personal information reflecting the changes in society.[171] This approach can be seen emphasising the accessibility and availability of information online, building on the fact that the everyday life to a larger extent happens not in parallel worlds, but in an intertwined, augmented physical world. Friendships, connections and social activities in social networks in the online world tend to be as 'real' as traditional counterparts, at least for the new eGeneration.

As Marhoof explains, by pretending to be one's real-world friend it is possible to trick someone into giving out personal information in Social Networking Websites i.e. online communication platforms, not limited only to websites.[172] But, one should realise that physical '*real'-world* friend is not in any sense more valuable or 'real' compared to a virtual-friend. That said, the problem is not related to the real-world/virtual-world dichotomy, but to the fact that adaptation to the new context is required where old rules, habits and practices may not apply. This idea can be best understood by comparing the 'pen-pal' to the 'net-pal'.You may not ever meet your 'pen-pal' or

169I. Lloyd, Information Technology Law, 5 (2011) [Information Technology Law]

170*See*, M. Albers, Realizing the Complexity of Data Protection *in* S. Gutwirth, R. Leenes & P. De Hert (Eds.) Reloading Data Protection Multidisciplinary Insights and Contemporary Challenges, 213 (2014)

171H. Nissenbaum, Privacy In Context: Technology, Policy, and the Integrity of Social Life, 195,231 (2010)

172A. Marshoof, *Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression*, 19 Int J Law Info Tech 110 (2011)

'net-pal', nor have any control how the pen-pal or net-pal uses the information you have given such as where you live and what your name is. You probably tell who you fancy, where you hang out or go to school, what were your biggest childhood secrets, and how old-fashioned and embarrassing your parents are. Yet, online you may use the technology for your benefit e.g. you have the possibility to track who processed your information whereas in the traditional context you may not have that opportunity. Also the negative consequences are greater. The differentiating factor is the context, the society we live in today, where irrelevant is whether the technology is 'good' or 'bad' but how, when and for what purpose it is used.

In the aftermath of World War II, the concept of human rights began to be recognized at an international level (e.g. Convention for the Protection of Human Rights and Fundamental Freedoms) laying the modern ground for the right to privacy; in the end of the twentieth-century Orwellian vision of surveillance in variety of forms threatened the privacy adding its feature to the concept of privacy; and after the tragic events of 9/11, Madrid 2004 and London 2005 attacks terrorism further shaped the concept of right to privacy.[173] The reflections of current and future society add the distinctive features *inter alia* the massive data flows and the central role of online information threatening the right to privacy.

2. Privacy in Case-law

As can be seen from case-law, the ePrivacy issues in law reflect the changes in society pretty accurately. The Case, ECtHR, *Malone v. the United Kingdom* in 1984[174] for example concerned the interception of telephone communication. This was at a time when privacy was seen from the perspective of an almost dystopic vision of Orwellian Society where 'Big Brother' carried out surveillance on its citizens and not only tried to control the speech and actions, but also the thoughts of its subjects.[175]

In the more modern case, ECtHR, *Konovalova v. Russia* in 2014,[176] the European Court of

173 Information Technology Law, supra note 169
174 *Malone v. the United Kingdom*, ECHR (1984), Series A, No. 82
175 For legal context of human rights and surveillance technologies *see, e.g.* B. Bowling, A. Marks & C. Murphy, Crime Control Technologies: Towards an Analytical Framework and Research Agenda *in* Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes, 57-59 (2008)
176 *Konovalova v. Russia*, ECHR (2014) Application No. 37873/04

Human Rights considered whether allowing medical students to observe a childbirth without the mother's explicit consent violated her right to privacy. Case introduces the privacy aspects that are related to consideration of different levels of privacy and information necessary for the purpose, as well as the specific and fine-tuned aspects of privacy such as right to privacy in some specific situation or condition, and finally rights to privacy that can be i.e. for women, but not for men for practical and obvious reasons.

The ePrivacy aspect is considered both in the CJEU, *Case 131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* i.e. 'Right to be forgotten' case[177] and in the proposed General Data Protection Directive,[178] where in both the ubiquitous nature of data and the empowering nature of regulation to manage personal data that is disclosed online and processed can be seen emphasized.

It can be learned from the case-law that privacy is all about balancing – against other rights as well as rights of the other individuals and society as a whole. Due to this the court cases supersede the regulation as a balancing method. This is because of the fact that the balancing of rights *inter alia* right of freedom of expression against the right to individual privacy is made case-by-case hence more appropriately made by a court than a regulator.

3. Role of Regulation in Protecting ePrivacy

Technology, law and privacy interactively shape how we define and undersand them. It can be concluded that shift is underway from 'fifteen minutes of fame' to 'fifteen minutes of ePrivacy'. This can be understood by considering the blurred boundary between private and public spheres in online world where personal data is published on a public medium. The 'fame' or publicity has become the 'new normal' in many way, whilst privacy in turn has become more scarce resource in online world.

The assumption can be made that, discrepancy between past and present requirements for regulation to protect privacy results from the fact that privacy has greater marginal utility today

177 *Case 131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] EU:C:2014:317

178 Data Retention Directive 2006, supra note 111

as economists would explain. Hence protecting privacy by regulation is more important than ever, not because people want more privacy than before either horizontally or vertically,[179] nor because protecting privacy by regulation is convenient, but because the value of privacy has grown significantly in the online world.

The role of regulation in protecting privacy can be seen very different compared to past for several reasons stemming from totally new dimensions of the concept of privacy – which can be coined by using the term ePrivacy.

4. Privacy in Different Contexts

The concept of privacy can be seen very context dependent.[180] What is perceived as private by individuals in offline world, can be seen public online or *vice versa*. Such information can be tangible e.g. income information, or intangible such as political views. What makes this problematic is the fact that same information that is available and accessible offline might not be a problem, but if it is accessible online it might become a problem. One simple reason is that the information can be combined with other information. Another aspect is the fact that information is made public without realizing it. An interesting practical example is 'Shodan', search engine that lets user find devices that are connected to the internet.[181] Any connected device such as refrigerators, SCADA systems, routers and web cams can be searched by anyone interested.

One's identity online may be different from the identity offline e.g. context specific personality and traces of past activity; or threats on privacy are not considered in offline world, but threats on privacy are seen everywhere in the online world. One of the reasons for this discrepancy in offline and online threats to privacy can be the public discourse, which effects how individuals orient themselves to risks.[182] In addition, the different legal notions, terminology and conceptions

---

179 *I.e.* wider scope of individuals private sphere, or certain personal information is seen more sensitive than previously and needs more protection *e.g.* geo-location.

180 P. Hiselius, *ICT/Internet and the right to Privacy*, 56 Scandinavian Stud. L. 201 at 203 (2010)

181 Search engines, such as Google, crawl for data on web pages and index it for users to find content. Shodan interrogates ports (FTP, SSH, HTTP etc.) and grabs the resulting banners *i.e.* meta-data the server sends back to the client, and indexes this meta-data for users to search nodes such as servers, routers and desktops.

182 *See*, M. Yar, Public perceptions and public opinion about Internet crime *in* Y. Jewkes & M. Yar (Eds.) Handbook of Internet Crime, 110 (2011) where it was also explained that individuals see risks mainly

of privacy may affect what is included in privacy e.g. private sphere as opposed to social or public sphere as in 'the theory of the spheres' emerged in German constitutional case-law.[183]

The privacy is not something than can easily be described by legal terms due to its dynamism and the fact that it is changing it's shape across time and space. The privacy is not limited anymore by physical boundaries i.e. home, family or even doctor-patient relationship, but privacy norms either positive or negative are also in force in public places and this can be achieved by technology,[184] or limited by technology e.g. face or speech recognition technologies. It can be argued that being public does not mean that the right to privacy does not apply or is impossible to achieve.

II. Present Law

The European Union, when ePrivacy considered,[185] is arguably one of the most significant front-runners in introducing several new ePrivacy related directives such as ePrivacy Directive,[186] eSignature Directive,[187] and regulation such as eIDAS Regulation[188] and proposed General Data Protection Regulation in ICT to provide certainty, trust and stability.[189]

The stability does not mean complexity but clarity, nor does it mean deregulation. It means that when in time of uncertainty there needs to be an applicable and enforceable law. This notion is pivotal in arguing on questions about proportionality and necessity for the goals to be achieved.

---

related to data security i.e. financial risks related to e-commerce, while public discourse on privacy concerns are eclipsed around moral issues.

183 *See, e.g.,* G. Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 24,25 (2014) on different degrees of private and Sphärentheorie.

184 *See* 'virtual net surfer patent' analyzed, EP2389641 - Einrichtung zur Generierung eines Virtuellen Netzgängers.

185 ePrivacy can be considered from variety of aspects such as law, technology and human rights

186 ePrivacy 2009 amendment, supra note 75

187 eSignature Directive 1999, supra note 91

188 eIDAS regulation, supra note 97

189 *See* Proposal for Data Protection Regulation (2012), supra note 102

1. Processing of Personal Data

Privacy in ICT is mainly enforced through directives in European level and traditionally the role of written law is more central than practices, concepts and principles created in case-law, hence the discussion revolves mainly around Data Protection Directive 95/46/EC,[190] and in a growing number around the proposal of General Data Protection Regulation.[191] Yet, case-law does provide practical examples where the legislation crystallizes into specific problems.[192] The impacts of regulation can be seen for example in lodgings of the application in data protection subject-matter initiating proceedings in the Court of Justice.[193] (See Appendix 2.)

In landmark case of 2003 *Bodil Lindqvist v Åklagarkammaren i Jönköping,* it was ruled that "Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46/EC."[194] The fact that the person who worked for the parish, wrote information about co-workers injured foot to a personal web page in today's context look like rather unharmful,[195] yet it must be noted that it is not only about privacy, but data protection in the sense that information of other person is used.[196] It can be argued that it is relatively common to post personal data such as location information or names of their friends as well as health information about colleagues in online communication platforms e.g in facebook status updates and WhatsApp messages. Considering the context, the real privacy challenges are in the accessibility and availability and in the fact that the information can be retrieved in the future for any different purpose than original i.e. how the information is used. When considering the

190 Data Protection Directive (1995), supra note 55

191 *See*, Proposal for Data Protection Regulation (2012), supra note 102

192 Encompassing overview on data protection case-law, inter alia Lindqvist, Volker, Innoweb, Google Spain, and relevant EU Law can be found in D. Solís, La Protección Judicial de los Derechos en Internet en la Jurisprudencia Europea (2014)

193 CJEU cases are available in 'InfoCuria - Case-law of the Court of Justice' – search in Court of Justice of the European Union web page and possible to classify based on subject-matter e.g. data protection. Available: http://curia.europa.eu/juris/recherche.jsf?language=en# Accessed: 22.11.2014

194 See the ruling *in Case 101/01, Bodil Lindqvist v Åklagarkammaren i Jönköping, [2003] EU:C:2003:596*

195 E. Kosta, Consent in European Data Protection Law, 228 (2013) [Consent in European Data Protection Law]

196 D. Manolescu, Data Protection Enforcement: The European Experience – Case Law *in* N. Ismail & E. Yong Cieh (Eds.) Beyond Data Protection. Strategic Case Studies and Practical Guidance, 225 (2013)

developments in using meta-data, e.g. patent on tagging communication artefacts and caching,[197] the information available from other sources than from a personal web page has exploded, but also the possibilities how it can be used.

Case 202/12 Innoweb v Wegener[198] can be seen as an example of more general EU regulation and enforcement trying to cope with advancements in emerging technologies in ICT, and possibly limiting the research and innovation, as CJEU ruling appears to suggest that better information search tools i.e. meta-search engines possibly as *a genus* are illegal in Europe.[199] Court can be seen to consider meta-search engines as a homogenous group of search engines, although the distinction from traditional search engines is rather artificial. The problem lies in the fact that also traditional search engines use meta-data. What is not yet considered by e.g. CJEU or Commission is how, in addition to the search engines allowing traditional searches based on indexing, searches from predetermined data collection; engines using meta-data; searches from data collection compiled by operator, or by end-users; and using several search engines simultaneously ought to be regulated if they are considered different.[200]

Another issue worth discussing is relatively surprising, yet almost too obvious considering the role of information, communication and technology in society. In Article 9 of the Data Protection Directive in relation to processing of personal data and freedom of expression it reads "member states shall provide for exemptions or derogations from the provisions[...] for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."[201] When considering this from a privacy perspective, almost any information may be subject to this exemption in certain conditions. It is a matter of balancing

197 *See,* patents EP2613499 and EP2513799

198 *Case 202/12 Innoweb BV v Wegener ICT Media BV and Wegener Mediaventions BV*, [2013] EU:C:2013:850

199 *Sui generis* database right, supra note 129. Here meta-data search engines as *a genus* is used in the meaning that in a taxonomy it is a category under all search engines.

200 *See* search.com as practical example. It performs simultaneous searches using other search engines such as Google, Blekko and Yahoo as well as allows end users to limit searches by slashtags and create own pre-determined databases. Search term 'privacy' results in news about privacy, wikipedia page and twitter privacy policy statement, whereas using slashtag 'privacy /law' search results are legal-encyclopedia, LexisNexis and Stanford Law Review which are clearly more personalized and beneficial for example legal researcher.

201 Data Protection Directive (1995), supra note 55

test. This is important regarding the role of individuals in journalism, blogs, first-hand videos, namely citizen journalism where normal citizens collect and process information, analyzes and reports information and 'upload' it to the internet or may provide it for the established media to publish it.

The fact that companies collect and process data is certainly not only a threat, but a high risk for privacy.[202] Another problematic area for regulation relates to companies having access to customer information through public-private partnership in the course of providing different services. Private companies providing public services can save cache or tag communication artefacts in a project including also data that is sensitive and customer as a data subject has unambiguously given their consent, but for some totally different purpose and use.[203]

Tagging artefacts i.e. creating meta-data that is hardly identifiable as a sensitive personal data, may regardless have severe risks to the individual or social environment such as friends and family. A more severe risk was the argument why certain categories of data are protected in a different way from 'normal' data, and among sensitive data according to Article 6 of the Council Convention No. 108,[204] which covers 'special categories of data'. Among these is for example sexual orientation, that can be easily argued being quite 'normal' and public information in many European Countries advanced in fundamental rights. It should be assessed whether the regulation should only cover the types of data, or also/only the *uses* of the data.

Article 6 of the Convention prohibits automatic processing of such data unless domestic law provides appropriate safeguards i.e. if appropriate safeguards in place, the processing is possible. Article 11 of the Convention sets minimum standards for the processing of these special categories, but it does not define these 'special categories of personal data' or what is meant by 'appropriate safeguards'. European Union regulation then gives a more specific explanation in Article 8 of the Directive 95/46/EC which sets out specific preconditions for the processing of

202 Threat describes the capability and intention aspect, whereas the risk describes the probability.

203 See for tagging communication artefact, Claim 1 of the patent EP2613499 and on data subject explicit consent Art. 8(2)(a) of the 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, which gives grounds for derogating from Art. 1 prohibition on processing personal data revealing sensitive data.

204 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe

sensitive data which apply in addition to more general rules on data processing in Article 6 and Article 7 of the Directive.

The default in Article 8 of the Data Protection Directive is prohibition, "member states shall *prohibit [*emphasis added] the processing of personal data revealing..."[205]. What is actually prohibited may be hard to define and understand in practice due to the word *revealing* used. The term *revealing* is to be understood, as Article 29 Data Protection Working party explains, "that not only data which by its nature contains sensitive information is covered by this provision, but also data from which sensitive information with regard to an individual can be concluded."[206]

Other consideration altogether is that whether the data processing is actually meant to be permissive, not prohibitive since as it is stated in Article 1 of the Directive "Member States shall *protect* [emphasis added] the fundamental rights and freedoms of natural persons," and "Member States shall *neither restrict nor prohibit the free flow of personal data* [emphasis added] between Member States for reasons connected with the protection...".[207] This view can be justified since for example the proposal for General Data Protection Regulation includes in addition to significantly more discussed 'right to be forgotten' largely unpublicized 'right of portability' which clearly allow a transfer of all data from one service provider to another upon request.[208] This means that data can be transferred from one service such as cloud service or social communication platform to another, and regulation applies to all companies processing the information of EU citizen. This can seen to limit risk of lock-in, but right of portability goes also far beyond simple interoperability. Further, more recent explanation was given in brief of *Amicus Curae* Jan Philipp Albrecht, *Microsoft Corporation v United States of America (2d Cir. 2014)* "The protection of privacy and personal data in EU law is not intended to stop the use and exchange of data. Its purpose is to regulate the transfer and storage of data, preserving the ability of the data subject to control his personal data."[209]

---

205 Data Protection Directive (1995), supra note 55, Art. 8(1)

206 *See*, Article 29 Data Protection Working Party, Advice paper on special categories of data ("sensitive data"), 6 (2011) [Article 29 DPWP on Sensitive data]

207 Data Protection Directive (1995), supra note 55

208 *See*, Proposal for Data Protection Regulation (2012), supra note 102, especially Art. 18

209 Brief of Amicus Curae Jan Philipp Albrecht on Microsoft Corporation v United States of America (2d Cir. 2014) Available: https://www.eff.org/files/2014/12/19/albrecht_microsoft_ireland_amicus_brief.pdf Accessed:

One aspect is to consider the threat to privacy associated with the processing of personal data in practice where life-time long information from one service is transferred to another service and the requirement for secure software code that exports the data from first service to the second should be standardized and 'privacy by design' principle in place.[210]

The presumptions may change and categorization of data seem to be relatively artificial, although it is necessary to differentiate sensitive data from 'normal data' for the purposes of regulation. But then the question can be made, what the purpose of regulation is. The categorization of personal data in Data Protection Directive[211] and the broad definition of sensitive data creates not only theoretical, but also practical problems. Photos taken by traffic surveillance cameras not only may, but in most cases do reveal information about 'racial or ethnic origin' or information about 'health' such as visible disabilities and should actually be considered as sensitive data if interpreted literally as defined in Article 8(1) of the Directive.[212]

It might be that what data falls under which special categories of data should be reviewed periodically or determined case-by-case.[213] This necessarily means that the role of case-law and soft law will get bigger. Practical implication of current law is that Article 8(3)[214] does not, in the absence of exception, allow the usage of health information in pre-schools or in performing a health insurance contract or the processing of sensitive information by legal practitioners since neither of these are 'health professionals'. In this sense, it is unacceptable that, to protect health and safety, it may create a situation even if only in theory that it is necessary to disobey the EU law. It must be noted, that 'explicit consent'[215] does provide possibility that prohibition in Article 8(1) may not be lifted,[216] but a new problem lies ahead.[217] It may be debatable that whether informed and explicit consent has been given i.e. individuals understand what they are

---

30.12.2014

210 P. Swire & Y. Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique,* 72 Maryland Law Review 335 (2013)

211 Data Protection Directive (1995), supra note 55

212 Data Protection Directive (1995), supra note 55

213 Category of sensitive data include trade-union membership whereas information such as geo-location and biometric data is not included, reflecting the context in which the Directive was drafted.

214 Art. 8(3) in Data Protection Directive (1995), supra note 5

215 Art. 8, para. 2(a) *in* Data Protection Directive (1995), supra note 55

216 Data Protection Directive (1995), supra note 55

217 Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), 8, 10, 16 (2007)

consenting; whether consent is free in cases where for example a person is in a critical condition or for some other reason is not given necessary information,[218] or does e.g. oral consent qualify as explicit.[219]

The outburst of sensitive information is because of the fact that our lives have moved online e.g. we communicate and express ourselves on social networks, we pay our bills and celebrate democracy by e-voting, and buy our clothes by means of e-commerce. Interestingly enough, Action 16 of the Digital Agenda for Europe concerns the issuing of a Code of EU Online Rights[220] summarizing the existing digital user rights in the EU in a clear and accessible way. The problem is that these rights regarding buying services and goods online are scattered across regulatory framework and due to the complexity of the framework online consumers are not aware of these rights. Further, if consumers are not aware of such Code,[221] does it serve the purpose since code does not remove the fact that privacy concerns or the lack of trust result substantially from dubiety. As Gavison points out: "Ultimately, the wish to have privacy must be in our hearts, not only in our laws."[222] This is partially yet to be discovered by European Union concerning the regulation on processing of personal data and protecting ePrivacy.

2. Trust

Two important applications of cryptography are digital signatures and encryption. Digital signatures can authenticate i.e. help to prove the origin of data, and provide integrity i.e. verify whether data has been altered, whereas encryption can help keeping data and communication confidential.[223]

---

218 Consent in ePrivacy related issues can be given by clicking the link, ticking the box or by electronic signature.

219 The term explicit consent has never been defined and explained, *see* Consent in European Data Protection Law, supra note 195

220 Code Of EU Online Rights. Digital Agenda for Europe. European Commission (2012) Available: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Code%20EU%20online%20rights%20EN%20final%202.pdf Accessed: 22.12.2014

221 Id.

222 R. Gavison, *Privacy and the Limits of Law*, 89 Yale L.J. 471 (1980)

223 K. Grewlich, Governance in Cyberspace. Access & Public Interest in Global Communications, 173 (1999)

The purpose of eSignature Directive[224] was to facilitate the use of electronic signatures and to contribute to their legal recognition by providing a legal framework for electronic signatures and certain certification-services for secure cross-border transactions.[225] Regarding other aspects of data protection member states must ensure that certification service providers and national bodies responsible for accreditation or supervision comply with Data Protection Directive 95/46/EC on the protection of personal data.[226] The eIDAS Regulation 910/2014/EC on electronic identification and trust services for electronic transactions in the internal market can be seen to contribute in legal terms to secure electronic interactions between businesses, citizens and public authorities.[227] Legislation team of eIDAS identified that, "the legal framework can create the impression that there are fewer legal safeguards than with physical interaction".[228]

European current regulation seems to find form and the scope is wide enough to cover all aspects necessary for knowledge-based society, cross-border eCommerce, private online services and online-buying as well as eGovernance services. But, As Neelie Kroes, the Vice-President of the European Commission responsible for the Digital Agenda said: "Services that are easier, more efficient, more convenient because they are online. But one thing is clear: people won't use what they don't trust."[229]

Problem lies in the fact that law is in place, but other societal aspects do have a significant affect on the outcome and efficacy of the law. Trust cannot be achieved by law, but not by technology either. Trust is essentially related to safety, familiarity and convenience which can be understood as a comfort zone, where an individual has control over personal data, personal space, right to opinion and expression, and trust that boundaries securing this personal space are not compromised or exposed, in which one of the essential features is privacy. If online is seen less

224 eSignature Directive 1999, supra note 91
225 Commission Directive 1999/93 of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures OJ 2000 L 13/12
226 Data Protection Directive (1995), supra note 55
227 eIDAS regulation, supra note 97
228 Electronic identification and trust services (eIDAS): regulatory environment and beyond, European Commission Directorate General for Communications Networks, Content & Technology. Available: http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond Accessed: 27.11.2014
229 N. Kroes,. *eID: unlocking confidence and convenience in a Digital Single Market*. The eIDAS Regulation Launching Event Brussels (2014) Available: http://europa.eu/rapid/press-release_SPEECH-14-690_en.htm Accessed 16.12.2014

secure than offline creating privacy concerns and risks, although these might be more perceived than actual problems, it does not mean that the fears of the individuals as such are not real. This situation should be turned into a source of motivation to create an even more secure and coherent eEurope, not a punitive or stigmatizing environment.

Even in Europe, it might be that in some countries the privacy can be significantly more highly valued than in others due to *inter alia* trust in government and economic or societal stability – the context can be the decisive factor. Emerging technologies such as the analyzed patent 'EP2389641 for System to generate a virtual web surfer' has been created to provide anonymity, which relates to hiding the identity whilst communication can be made as public as possible, or to provide seclusive privacy i.e. communication, personal and private information is not made public.[230] These technologies can not only complement the regulation in place but make it possible in practice by building sense of trust and safety.

The 'additional safeguards' in Data Protection Directive[231], are rather vaguely defined. As explained "The Directive in its current approach does not contain any specific rules on the security of processing sensitive personal data which would go beyond the general requirements on data security in Art. 17 of the Directive. Currently it may therefore appear that sensitive data are in practice no more protected than data that does not fall under this category."[232] Legal as well as technological safeguards should be defined in more detail, given that the purpose is to provide more protection when sensitive data in question. In claim 1 of the Patent EP 2389641, invention relating to virtual web user, it is mentioned that the traffic data relating to users is encrypted with different keys. In description it is mentioned that by transformation system it is excluded that the operator can be in the role of a 'Big Brother'.[233] These means provided by emerging technologies in ICT can be used in addition to legal safeguards to reinforce ePrivacy rights especially when sensitive data considered.

---

230 It can be argued that in current ePrivacy context, privacy doctrines built on seclusion are not addressing the implications of emerging technologies. Actually 'privacy in public' should be concentrated on due to fact that the seclusive privacy is not possible nor desirable if individuals wants to be an active citizen and participate in society.

231 Data Protection Directive (1995), supra note 55

232 Article 29 DPWP on Sensitive data, supra note 206, at 11

233 *See,* patent EP2389641, Description [0022] "Es wird im Prinzip ausgeschlossen, dass dem Betreiber die Rolle eines "Big Brother" zuwachsen kann, die somit weitgehend obsolet wird."

Above-mentioned considerations also introduce the aspect of personal responsibility which is absent in large extent in current quarter-century-old privacy regulation in EU.[234] To large extent this is due to fact that only after the emergence of the online world possibilities, certainly not to keep everything private, but means for example to see who has processed personal information and for what purpose, is possible. To understand this aspect might actually add to trust since individuals have a sense of control and may actively start evaluating trade-off i.e. what to get in exchange for giving information. However, this does not mean that the burden is on the individual, it's that EU should rather provide means for individuals and empower them to protect ePrivacy. Technological safeguards should be considered as additional safeguards, but not only because of their technological features relating to privacy, but considering the social aspects and trust, if individual has a tangible built-in (technological) solution to control personal data, the trust on these online services is likely higher. In addition, if individuals use these user-friendly solutions, it contributes to the habitualization and *ipso facto* trust.

3. Developing Law by Introducing new Principles and Concepts

a) Right to be Forgotten Principle and Case Google Spain

Considering the concept of ePrivacy, the right to be forgotten, in Article 17 of the proposed General Data Protection Directive,[235] is very distinct from the right to privacy. This is due to the fact that protecting privacy relates traditionally to information that is not publicly known or shared, whereas the right to be forgotten involves removing information that is publicly known, and the intention is to limit the third parties to access the stored information which is already made public.[236]

In an attempt to go beyond common and generally shared views, it might be possible to argue that the Court in its Judgment in *Case C 31/12, Google Spain* in attempts to cement the Right to be forgotten principle, might be too extensive, although, the conflict between rights such as 'right

234 K. Nyman-Metcalf, Lectures in Legal Framework of e-governance (2014) [eGovernance Lecture Notes]

235 Proposal for Data Protection Regulation (2012), supra note 102

236 'Privacy in public' should be considered, *see, e.g.,* H. Nissenbaum, *Toward a Approach to Privacy in Public: Challenges of Information Technology,* 7 Ethics Behav 207 (1997)

to freedom of opinion and expression' which includes freedom to seek, receive and impart information and ideas through any media and regardless of frontiers, and right to privacy is not necessarily detrimental to the survival of either.[237] However, in practice it seems that they may be detrimental for all rights balanced. The right to be forgotten ruling applies only to Google's local European sites meaning territorial restriction in applicability. It follows that the regulation and judgment is currently easy to be circumvented by *users* by conducting search on Google.com through which the information is fully available in search results and publicly stored data in original source is accessible easily by clicking links. This means that the EU competence and applicability of the right to be forgotten is very limited in practice for now, yet the information is not freely or equally available, not to mention that the information that is removed may attract even more publicity.

Taking into account the nature of the internet, it is easy to think several other problems such as information may relate to other persons who want the same information to appear. On a statement published on 26th November 2014, the Article 29 Data Protection Working party[238] it says that "Under E.U. law, everyone has a right to data protection," and that "E.U. law cannot be circumvented."[239] Enforcement of the guidelines[240] What is not discussed to the authors knowledge, is that respecting the right to data protection and ePrivacy is not fully incorporated if only links in search results under certain conditions can be requested to be removed.[241] This is ineffective yet lays another burdensome obligation for search engine operators.[242] The indexing,

---

237 Art. 19 of the Universal Declaration of Human Rights. the General Assembly of the United Nations (1948) For general discussion on striking a balance between rights and freedoms, *see* S. Coliver, K. Boyle & F. D'Souza, Striking a Balance. Hate Speech, Freedom of Expression and Non-Discrimination (1992)

238 Article 29 Working Party set up under the 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

239 *See*, Article 29 Data Protection Working Party press release, Adoption of guidelines on the implementation of the CJEU's Judgment on the "right to be forgotten" *(*2014a) Available: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20141126_wp29_press_release_ecj_de-listing.pdf Accessed: 26.11.2014

240 It must be noted that guidelines are not binding since Article 29 Working Party has advisory status and acts independently.

241 Individuals may ask search engines to remove links in search results with personal information where information is inaccurate, inadequate, irrelevant or excessive for the purpose of data processing as mentioned in the para. 93 of the ruling *in Case 131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* [2014] EU:C:2014:317

242 The 'controller' is "natural or legal person, public authority, agency or any other body which alone or

third party or persistent cookies, cache or any other form of storing the data should be considered based on analyzed patents if the protection of sensitive personal data is the objective and a more coherent view is to be created. Current situation only adds to legal uncertainty and businesses are pushed to find practical solutions to circumevene the prohibitions possibly creating new threats. In the course of pursuing the aim to protect the right to privacy and the protection of personal data of individuals, the obligations for search engine operators seem to be more than anything else collateral damage or expression of determination,[243] since the right to be forgotten may be to simply establish that search engine operators qualify as data controllers and are different from original publishers,[244] rather than to create more coherent approach to protect ePrivacy.

b) Standardization and Privacy by Design in Proposed Data Protection Regulation

It is not to argue against the benefits of harmonized regulation, but the over ambitious objectives might prove impossible to achieve through introducing new legislative instruments. Although, the technological data protection safeguards in ICT are not a new idea since already Data Protection Directive 95/46/EC called for data controllers to implement technology safeguards in the design and operation of ICT *inter alia* Recital 46 calls for "protection of the rights and freedoms of data subjects", and "with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself".[245]

---

jointly with others determines the purposes and means of the processing of personal data" *See* Data Protection Directive (1995) supra note 55, Art. 4(d). Other obligation for data controllers is inter alia duty to notify data breaches within 24 hours to the Data Protection Authority under Article 31 proposed Data Protection Regulation, *see* Data Security Breaches and Privacy in Europe, supra note 71, at 25

243 For limited impact of de-listing, *see* Article 29 Data Protection Working Party guideline, Guidelines on the implementation of the Court of Justice of the European Union judgement on 'Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/121 (2014b) Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf Accessed: 26.11.2014

244 Id. The respective legal grounds of original publishers and search engines are different e.g.search engine should carry out the assessment of the different elements such as public interest, nature of the data and actual relevance. This derives from the fact that the universal diffusion and accessibility of that information by a search engine, together with other data related to the same individual, can be unlawful simply due to the disproportionate impact on privacy.

245 Data Protection Directive (1995), supra note 55

The proposed General Data Protection Regulation[246] can be seen as the step towards the right direction removing the complexities, yet some concerns remain. The privacy by design (PbD) in proposed data protection regulation in its current form may be seen in conflict with the fact that majority of business models in the future are build around data processing, using cloud computing and Big Data. So instead of simply passing on the legacy of Directive 95/46/EC being very precise,[247] if PbD is to be introduced in practice, it should be a consistent concept including all the stages starting from the acquisition and public procurement of ICT.

A suitable measure in combination with binding principles might be positive incentives and standards to maintain a certain minimum level of security, data protection and to foster the introduction of PET's allowing to better control the personal data by engaging all stakeholders at all levels. It is evident that to introduce PbD, in addition to legislative instruments, regulatory framework to be effective, policy framework and ICT standards that take into account the technology convergence are necessary. It would mean that all the current private services such as online social platforms, search engines; public services such as ID-cards, eVoting and traffic control; access points such as tablets and IoT; cloud services with encrypted data and secure access; and RFID technologies, WIFI-routers etc. has to comply with the regulatory framework.

If a variety of new obligations are introduced, the effectiveness of the most central ones may suffer and be detrimental to the future European 'digital agora'. The proposal for Data Protection Regulation does not define or give any references for definitions or explanations what the technological solutions of PbD are, but is empowered “to adopt delegated acts [...] for the purpose of further specifying the criteria and conditions for the technical and organisational measures[...] in particular taking account of developments in technology and solutions for privacy by design and data protection by default”.[248] This creates possibilities for data processors and other businesses to define the concept and invent their own measures and technologies which may provide only the minimum level of data protection on their own terms blurring the limits of the right to privacy and data protection in online world. Consequently, this development may lead to the situation where it is even more difficult to secure right to privacy or data protection by legislation due to fact that it might require to intervene and enter to the business

246Proposal for Data Protection Regulation (2012), supra note 102
247Data Protection Directive (1995), supra note 55
248*See, e.g.,* Art. 30, para. 3 *in* Proposal for Data Protection Regulation (2012), supra note 102

sphere and private information which is hardly possible nor acceptable.

To innovate regulatory framework by introducing new principles and means is very welcomed and should be endorsed. Although, if the concepts are not defined or fully understood; the scope is extended not only to data controllers but to other parties such as engineers and technology designers; impact assessments are not done after the adoption in practical level how to comply with these relatively vague provisions; and finally regulation does not in practice enable the adoption of regulation for specific technological context, the results may turn against what is intended to achieve.[249]

The positive side of privacy enhancing technologies (PET), the embodiments of PdB in practical level, is the end-to-end protection since if the privacy and data protection is embedded into the design and architecture of the IT system, from the individuals perspective, the functionality and user-friendliness remains since protecting privacy does not require additional actions from the user as it is the 'default option'.[250] Privacy risks, usually due to human actions, can be significantly reduced by standardization. Future interplay with law, technology and privacy is getting more complex, and may require detailed level guidelines, communications, and best practices, namely soft law, but as several flagship initiatives of the Europe 2020 strategy underline the importance of voluntary standardization.[251] This development of using specialized knowledge and expertise in the guidance of European Commission can be seen very promising from the perspective of protecting ePrivacy in ICT.

To sum up, the privacy by design as a principle should be understood not only as a legal principle. It should be introduced as an interdisciplinary approach, voluntary cooperation as a central feature in standardization by *fora and consortia* e.g. World Wide Web Consortium (W3C) and Internet Engineering Task Force (IETF).[252] National regimes such as German renewable

---

249 *See* Article 29 Data Protection Working Party & Working Party on Police and Justice, 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. (2009) Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf Accessed: 27.11.2014

250 S. Perry & C. Roda, Teaching Privacy by Design to Non-technical Audiences *in* F. Cleary & M. Felici, Cyber Security and Privacy: Third Cyber Security and Privacy EU Forum, CSP Forum 2014, Athens, Greece, May 21-22, 2014, Revised Selected Papers, 121 (2014)

251 Commission Implementing Decision of 31 October 2014 on the identification of Universal Business Language version 2.1 for referencing in public procurement, OJ 2014 L315/44

252 Fora and consortia have become established as leading ICT standards development bodies, and the PbD and other principles may be introduced more effectively by voluntary standardisation than by

energy regime can act as a benchmark from totally different context, yet relevant introducing the importance of interaction, education and overall approach.[253]

4. The Big Data and Public-Private-Partnership

The emerging technologies create new business opportunities and for the benefit of common digital market, market needs companies from which individuals can buy private but also public services. It is challenging to strike the balance between legal measures such as restrictions or large punitive fines whilst simultaneously supporting future economic growth and welfare in the Europe. The data sector is growing by 40% per year, and Big Data is seen by Commission as one of the Europe's key economic assets giving European industry a competitive advantage in global level.[254]

One of the features of Big Data is that sensitive personal data or data that can reveal sensitive information are not possible to separate from personal data when the volume is huge, hence the data on which for example profiling is conducted, may include sensitive personal data which is originated from communication and information sharing during Public-Private-Partnership (PPP) either using public ICT in private sector such as digital ID card for identification, or private bank developed identification to identify citizens for public services.[255]

The analysis on future technologies points clearly to the fact that the storing of data and future use is the growing concern, and to respond to these issues, the future use aspect should be considered in a more detailed level. For example when government eServices are build in

---

legal instruments. *See* the Communication from the Commission entitled 'A strategic vision for European standards: moving forward to enhance and accelerate the sustainable growth of the European economy by 2020' (2011) recognizing the specificity of ICT standardisation where ICT solutions, applications and services are often developed by global ICT fora and consortia that have emerged as leading ICT standards development organisations. Available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52011DC0311 Accessed: 19.12.2014

253 For more information on German renewable energy regime, *see* "European renewable energy incentive guide – Germany", Global Legal Practice Norton Rose Fullbright (2013) Available: http://www.nortonrosefulbright.com/knowledge/publications/66180/european-renewable-energy-incentive-guide-germany Accessed: 18.12.2014

254 *See*, European Commission press release, *European Commission and data industry launch €2.5 billion partnership to master Big Data* (2014) [PPP on Big Data] Available: http://europa.eu/rapid/press-release_IP-14-1129_en.htm. Accessed: 7.12.2014

255 eGovernance Lecture Notes, supra note 234

cooperation with private businesses the level of access to information and the necessity to process the personal data should be controlled.[256] The risk is that private companies can use the data achieved for other purposes or combine it with other data.

The role of information as an intangible asset is growing in importance for companies, but the development is similar in the public sector. Big Data and geo-location can be used to promote traffic safety, to create intelligent cities, and to provide individual- or group-targeted services. This development of Big Data and PPP was embodied when European Commission signed a Memorandum of Understanding with Big Data Value Association representing several European companies inter alia Nokia Solutions and Networks, SAP and Siemens to develop Public-Private-Partnership on Big Data.[257]

256 There are several technological solutions to retrieve only data necessary for the purpose e.g. to confirm the identity of the driver during traffic control activities excluding all other irrelevant information. It might be also possible to introduce task-specific software agent that has 'self-destruction mechanism' for destroying the information retrieved after specified time to limit the unnecessary storage of data.

257 PPP on Big Data, supra note 254

E. Conclusions and Recommendations

I. Conclusions

1. New context, New Threats, New Approach

Current European regulatory framework is partially unable to respond to the new privacy concerns in the online context by emerging technologies in ICT although several new principles and concepts have been created. As Charles de Montesquieu noted, "Les loix inutiles affoibliffent les loix néceffaires" – useless laws weaken the necessary ones.[258] Specific requirements of data protection may guide the focus and discussion on areas that are particularly susceptible to interference with right to privacy, but the risk is that the overall view is lost.

The future risk is that in transformation from directives to regulations unnecessary regulatory burdens are adopted partially by accident, resulting in more restrictive regulation. This may happen due to not taking into account that even in situation where content of instrument does not change *de facto*,[259] the difference between features of legal instruments create, *ipso facto*, more restrictive framework.[260] This is alarming in a sense that the more coherent, yet enabling regulatory framework should be created which takes into account the emerging technologies and

258 C. Montesquieu, De l'Esprit des Lois, 266 (1772)

259 *See, e.g.,* Art. 8(1) in current 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 (1995) on special categories, and Art. 9 of the proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2012)

260 This notion is based on research conducted in this thesis, where it is visible that in current reform directives such as 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 and Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures are replaced (or expected to be replaced) by regulations*, see, e.g.,* Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

the future aspect i.e. legal certainty.[261]

What is notable in the *joined Cases 293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and *594/12 Kärntner Landesregierung and Others,* is that it was found that European Union legislature has exceeded the limits imposed by compliance with the principle of proportionality and purpose limitation implicating that EU was in the *cul-de-sac* in balancing the fundamental rights and exceptions and derogations from the rights. New course needs to be taken, but whether it is by interpreting existing regulation, introducing new or solved by technological solutions is to be seen.[262]

What is necessary is to concentrate on the real issue which is in growing number, not the collection of data, but how it is used and for what purpose. Considering the studied patents, general conclusion can be that it is rather unimportant to try to prevent giving any personal information, but when you make personal information available, what is the relevant information and what services you get for that. The balancing is hence also on the individual level. It is significant whether the services are beneficial for the individual and on what cost. This aspect is important in considering what might be the new approach in protecting privacy in ICT.

Currently one of the main feature creating problems in practice is "[f]ragmented and overly complex legal environment".[263] Although complexity is the most obvious and well known concern, it is very challenging to solve and there is no 'punch line' truth, especially considering the fact that the regulatory framework is developed to a very advanced level in many fields based on an old context and a new approach is challenging to adopt.

Objectives of the policy-making are not achieved partly due to lack of uniform legislation and

---

261 Commission acknowledged the complex and burdensome regulatory framework and started to cut red tape already in 2007 with Action Programme on Reducing Administrative Burdens(COM/2007/0023 final), and with the new approach of Smart Regulation and the launch of the REFIT Programme (COM/2012/746 final Commission as a whole have initiated a fundamental change in the EU law-making process. *See*, final report by High Level Group on Administrative Burdens, *Cutting Red Tape in Europe* (2014) Available: http://ec.europa.eu/smart-regulation/refit/admin_burden/docs/08-10web_ce-brocuttingredtape_en.pdf Accessed: 20.12.2014

262 Example on simple yet effective technological solution is the IPV.6 when internet addresses were running out. Other means would have been to introduce new law or policy such as how many addresses you can own at a time or for what purpose. This would not have contributed to the objective solely, but introduced unnecessary collateral damages for businesses and individuals.

263 *See*, European Commission press release, *Commission urges governments to embrace potential of Big Data* (2014) Available: http://europa.eu/rapid/press-release_IP-14-769_en.htm Accessed: 16.12.2014

interoperability[264] within legislation.[265] In other words, the system has everything, but due to the gradual development of EU law in relevant law regarding ePrivacy in ICT, the conclusion drawn is that structure of the European regulatory framework should be simplified to achieve coherent legal framework, and leave possibility for soft law on specific issues.

Several legal researchers are concerned that unless the tendency to enact narrowly framed legislation is minimized, the possibility for further legal problems as technology continues to evolve is high.[266] Some of these assumed problems can be mitigated by more innovative and flexible alternatives such as introducing temporary legal measures in addition to more general legislation. Other possibility worth considering is to achieve the objectives of legislation by technological means, that is either complementing the law by making it possible to achieve the objectives in practice, or using the technological solution as a substitute i.e. PETs. Doing so, the efficacy of European regulatory would most probably follow.

2. Legal Certainty and Protecting ePrivacy

In coming up with new concepts, principles and legal measures, the effective and up-to-date regulatory framework is essential to ensure ePrivacy rights, but the *vacatio legis* principle should be respected i.e. time for businesses as well as individuals to adapt and comply with new

---

264 Word interoperability is used instead of interaction to emphasize the fact that it is not enough to only take into account primary or other secondary law, but to consider as an entity to form a coherent framework and create legal certainty. Consider interoperability in current European regulatory framework between fundamental rights that are to be protected, Primary law securing these rights and Directives such as invalid 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.

265 Considering for example the development of one-stop-shop ideology. As the former (Věra Jourová took the post of Justice, Consumers and Gender Equality in 1 November 2014) EU's Justice Commissioner Viviane Reding said "The message the European Parliament is sending is unequivocal: This reform is a necessity, and now it is irreversible. Europe's directly elected parliamentarians have listened to European citizens and European businesses and, with this vote, have made clear that we need a uniform and strong European data protection law, which will make life easier for business and strengthen the protection of our citizens". S*ee* European Commission Memo 14/186 *Progress on EU data protection reform now irreversible following European Parliament vote* (2014) Available: http://europa.eu/rapid/press-release_MEMO-14-186_fi.htm Accessed: 16.11.2014

266 *See e.g.* Sui Generis Rules, supra note 13

regulation.[267] However, this does not mean that businesses should not sometimes be forced to comply with legislation, or sector specific regulation in protecting ePrivacy.

Existing law should also cover technologies and implications which are yet unknown. Challenging is the fact that technological development creates perceived risks to privacy, but also real threats. These new threats however may also be created by introducing law that is intended initially to protect the right to privacy or to protect the data, yet simultaneously causing legal uncertainty. The defining feature why technological uncertainty i.e. emerging technologies and disruptive forces are seen beneficial but uncertainty in regulation negative, is the fact that fundamentally the role of technology is to introduce change and invent, whilst the role of law is to create stability.

It requires understanding of technologies to create specific regulation, but especially to be able to introduce legislation that is effective yet not disproportional. Predictable and acceptable, yet taking into account the new threats. The solution may also be balanced combination of several measures and new aspects such as temporal scope based on the status of the market in question or horizontal scope i.e. balancing *sui generis* regulation and technology neutrality.

Legal certainty in ePrivacy context means not only the certain central requirement in 'nomocracy' that subjects to law should be able to regulate their conduct, although it is the starting point that law is in place and legal development follows certain path. The emphasis is on the fact that there needs to be right balance between stability and flexibility. This introduces the possibility to have simultaneously enabling, flexible as well as foreseeable regulatory framework.

3. Adequate Legal Measures

Regulation is a question of combination and balance of several suitable and relevant measures. Therefore, although current European regulatory framework, including hard law such as

267 *See* especially *Case 131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, [2014] EU:C:2014:317* and the right to be forgotten principle which changed the role of search engine operators cementing them to be data controllers in the meaning of Art. 2(d) of the 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; the introduced privacy by design principle; and expanding the provisions beyond data processors.

directives and soft law i.e. quasi-legal instruments, is useful to outlaw the worst practices, they are bound to be limited in promoting effective improvements of ePrivacy in ICT. It can be argued that in a situation where the rights of individuals and harmonization of laws need to be balanced, regulation is already in the wrong track. This can be seen as a one problematic issue in the European regulatory framework. Intangible ideas need to be transformed into tangible form. Right to privacy needs to be provided in practice since privacy law fulfills its purpose only after rights are achieved in practice.

The harmonization should be achieved in the level of minimum standards and goals, not considering the means how to reach that common goal in different member states. One member state may have the real access to internet, whereas in another country the access to internet is not even possible due to lack of infrastructure. As an example, the recent statistics on information society released on October 2014 revealed that at regional level in Europe there were 26 regions where at least 35 % of the population had never used a computer such as nine regions in Italy, and in a region, Sud-Muntenia, in Romania majority of the population had never used a computer.[268] Whereas in several regions in Denmark, the Netherlands, Finland, Sweden and the United Kingdom 98 % of the population had used a computer.[269] Based on these facts the context based approach would be more effective, and harmonization of laws should be seen as a secondary goal or as a mean for achieving the objective.

One-stop-shop can be seen as one of the important aspects in developing adequate legal measures considering the fact that businesses have to deal with only one authority, but also that individuals have the same opportunity by the growing role of national Data Protection Authorities (DPAs), and National Regulatory Authorities (NRAs) in general. Although, rather disappointingly the majority of the justice ministers on 5th December 2014 in a Council meeting rejected that businesses should deal with only one DPA in Europe.[270] The general architecture

268 The statistics reveal that the Digital Divide in the access level has not been mitigated, problems exist in real access i.e. but also the new Digital Divide in the speed and quality of access to internet has emerged. See European Commission, Eurostat regional yearbook 2014. Eurostat statistical books, 173 (2014)

269 Id.

270 Council of the European Union, Main results of the Council, 3354th Council meeting Justice and Home Affairs (2014) Available: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/146049.pdf. Accessed: 6.12. 2014

was endorsed where only in the most important transnational cases the one-stop-shop mechanism is introduced leading to unnecessary complexity where in the most cases several DPAs get involved.[271]

When not considering the general approach, but specific ePrivacy related ICT law, sometimes more strict legal instruments should be preferred. Such is the case with identification regulation i.e. 1999 eSignature Directive[272] and the eIDAS Regulation.[273] What is notable, is that the old legal measure was a directive, and the new is regulation. It is hardly an accident that directive was replaced by regulation, and it can be said with high confidence that the change in legislative instrument was to provide harmonized and coherent regulatory framework.

4. Flexible Framework, Stronger Rights

As Hustinx notes, two lines of development in the European regulatory framework can be identified, attempt to make privacy and data protection rights stronger, and ensuring a more consistent application of those rights across the EU. In order to achieve these two, they should be developed simultaneously[274], otherwise neither will be achieved or in expense of ePrivacy rights.[275]

Finally it must be noted that if Hustinx is right in predicting that new regulation on data protection will bring much greater consistency, as well as allowing flexibility for interaction with national laws,[276] the research question "Can a general approach on how to respond to privacy threats be recommended by analyzing specific implications of emerging technologies?" can be answered by saying that a general view can be made, and it is at least partially in accordance with the European regulatory framework hence possible to implement. Threats needs to be responded by coherent regulatory framework, which is supportive, not restrictive by its nature.

---

271 Id.
272 eSignature Directive 1999, supra note 91
273 eIDAS regulation, supra note 97
274 See the recommendation on introducing a Car Pool Lane for data protection regulation
275 P. Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, 50 (2014) Available: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf Accessed: 26.11.2014
276 Id, 51

Challenge lies in the fact that, to respond to threats or actualized risks that are related to specific technologies and are totally new, law should be absorbant and possible to adjust depending on the case and context within certain predetermined limits; and effective to force subjects of regulation when necessary. The efficacy of regulatory framework can be found from the right balance of these features in responding to ePrivacy threats in online world.

Specific feature of ICT is that the regulation in certain aspects should be preferred over directive since it needs to be adopted as such as a part of national legislation to be effective. In addition conclusion based on emerging technologies and analysis on the European regulatory framework can be made that data protection and ePrivacy can be seen to be even more important in the future, considering digital markets, cross-border identification, encryption in online transactions and e-commerce. This leads into the conclusion that future legislation on ICT is certainly more based on regulations that directives. For example eIDAS 910/2014 is a regulation, not a directive as is the eSignature Directive 1999/93/EC which it is going to replace. This can be seen indicating the general development in the European regulatory framework of ICT becoming more important and move towards the core priorities of European Union i.e. too important to be dealt by market or member states implementation.

This development can be at least partially due to the fact that regulation is a more suitable measure when certain technologies will be considered as a critical infrastructure (CI) or as a part of other CI.

Conclusion can be made that ICT is not a homogenous group of technologies which should be regulated in certain way, but ICT is very context dependent. In general the directive should be preferred since it is less intrusive, but what is in the core of EU principles and interests it is more effective to have regulation.

To answer to the research question, “How does the current European Regulatory Framework for ICT respond to new ePrivacy threats?”, general conclusion can be made that, although EU acts in *bona fide* and objectives are valuable, current European regulatory framework concentrates, or to be more precise, is interpreted to excessively emphasize prohibitions; creates principles or concepts without defining them; and uses formal approach and 'command and control' methods.

It may be that in certain fields current regulation can be even detrimental to the objectives.[277] Objective is not to achieve right to privacy on paper, but in practice. As it is in the intellectual property law, one of the requirements for invention to get the protection is utility requirement i.e. industrial applicability. Invention can be considered worth something, only if it has some practical implementation. This can be understood in regards to ePrivacy in ICT law by noting that the ePrivacy and data protection regulation is worth something only if it can protect ePrivacy in practice. Purpose is not to have network of laws, but to protect fundamental rights of the individuals.

II. Recommendations

Although the current law lays the playing field on which regulators and courts operate, it does not mean that the thinking is limited to these boundaries. Hence the aim is to propose recommendations *de lege ferenda* on the protection of ePrivacy in ICT context.

In general, all presented recommendations share the idea that regulating technologies need interdisciplinary cooperation and specialized understanding of technologies to determine the best legal instruments, regulatory means and most appropriate level of regulation. A very fundamental notion is that the internet is mainly private-sector led, and the technology and tools for access to internet are provided by private companies. The role of public-private partnership in providing public e-Services is pivotal. In addition, many technological standards as well as internet codes of conduct are set and maintained by non-governmental organizations. But to further develop laws and regulation in general, the role of government is essential in gathering all different stakeholders around the same table, and without political will, changes do not happen.

The subjects of regulation are the ones who enable (businesses) or accept (individuals) the means i.e. eGovernance, eCommerce and all relevant technologies. But, what is essential to note, is that those are only the means to an end. The 'end' is eDemocracy where the protection of fundamental rights and rule of law are its features. The role of European Union can be seen to create enabling regulatory framework for this purpose on offline as well as online.

277 One such example can be the European approach to reverse engineering where PETs are developed and online security and privacy companies try to reverse engineer the malicious software.

Finally the importance of context cannot be emphasized enough. As Solove pointed out, “We cannot ascribe a value to privacy in the abstract. The value of privacy is not uniform across all contexts. We determine the value of privacy when we seek to reconcile privacy with opposing interests in the particular situations.”[278]

1. Sensitive Personal Data

In contrast to the special categories of sensitive data listed in Article 8(1) of the Data Protection Directive 95/46/EC, in proposal for General Data Protection Regulation the generic definition of sensitive data should be included, but member states should be able to decide the specific categories what should be listed or not listed. For example 'trade-union membership' should be removed from the list in most countries whereas ' geo-location data' may be included. If the regulation is preferred over directive, it is of even more importance how these kind of lists appear in the regulation.

For example the Article 8(1) in current Data Protection Directive: “member states shall prohibit the processing of personal data *revealing* racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life”, should be changed. The new form in e.g. proposal for a General Data Protection Regulation can be as such: “member states should *protect individual's* sensitive personal data when personal data is processed. Sensitive Personal data is personal data which are *capable* by their nature or by the *context* in which they are processed of infringing fundamental rights of the data subject or *any natural person*. M*ember states may lay down categories* of sensitive data where the conditions set in this directive are met.“[279]

This recommendation emphasizes the fact that 'Article 9 Processing of special categories of personal data' should not repeat the problematic aspects of the Data Protection Directive. By passing the content into the Regulation it might actually prove to be even more problematic than

278D. Solove, Understanding Privacy, 87 (2008)

279As the name of the directive indicates, the objective is to explicitly protect individuals. Hence the wording in this suggestion is changed correspondingly. The fundamental rights of data subject but also the rights of other individuals on whom processing of sensitive data may have discriminative or similar effect should be considered.

previously considering the differences between directive and regulation. A regulation is binding in its entirety, self-executive and directly applicable in all member states, whereas a directive leave to the national authorities the choice of form and methods.[280] In addition to the aforementioned proposal, it might prove to be sufficient to have in subsequent paragraphs exemptions set such as on consenting, as well as possibly exemption regarding the scope within which member states may take the specific context into account.

2. Car Pool Lane Approach

The leading idea of the 'Car Pool Lane' approach is that it guides to consider 'market effect' by direct impact assessment on and by the participants and the subjects to regulation after new law is implemented, not only during the 'regulators sphere', but during the 'subject sphere'.

It also enforces the transparency of regulatory work. It is intended to take into account several levels – primary law i.e. human rights;[281] secondary law i.e. possible conflicting interests of legal instruments; and practical level. If the effects of new regulation are not considered after the implementation, the objective may never be achieved and initial purpose of law is lost in the process.

The idea of a Car Pool Lane is to get faster to the destination by using the lane which can be used only if there are two or more passengers. In a regulatory context, this means that the objective is first defined such as 'Welfare of the European Citizens and Economic Growth'. Secondly, the projects and developments from connected fields across disciplines are identified which contribute ultimately to the same shared objective. Thirdly, the process is done gradually in

280 For the legal basis, *see* Art. 288 of the Treaty on the Functioning of the European Union.

281 Already in 2005 when 'Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005, was made public, it was noted that imposing the data retention obligations on communication service providers without having first realised adequate, specific safeguards is not to be accepted within the existing European legal framework, and to find if there are less privacy-intrusive approaches not undermining individual human rights including the right to data privacy. *See, e.g.,* Article 29 Data Protection Working Party, Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005) Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp113_en.pdf Accessed: 16.12.2014

steps, considering the implications of selected most suitable legal instruments and adjusting accordingly.

In European Union terminology this can be understood, by an example from Digital Agenda context: 'vibrant digital market' is achieved by removing the blocks for free flow of online services by 'Fast and ultra-fast Internet access'. Although, it may be irrelevant to make advancements in 'Fast and ultra-fast Internet access' if the certain level is first achieved in 'Trust and security'. To make any relevant progress, the 'Enhancing digital literacy, skills and inclusion' should be developed first and the impact assessment should be done, and proceed accordingly in other areas.

In simplified terms rather than using several different 'cars' and arriving at different times without a clue of the process of the other relevant projects, the Car Pool Lane provides flexible approach, yet resulting in more coherent and effective regulation.

To consider the digital divide as an example to prove the point, although research has been conducted, it drew attention to technology diffusion in the 1990's, and later on internet usage e.g. basic skills and content.[282] Yet it lacks in addressing the most relevant issues related to not only accepting and trying eTechnologies, but to habitualization i.e. the regular use in all aspects of every day life over time. Also new divides appear to create new concerns to e.g. net neutrality. Then simply having an access is not enough, but the speed is also a concern since the new content requires faster connections.[283] But, to respond to these issues the problem field needs to be considered as a whole including adequate legal instruments and regulatory measures.

When comparing the differences in member states by taking into account cumulative effects, the digital divide has widen in terms of impacts as the benefits of ICT's increasingly permeate all different activities.[284] ICT Law may be the field of law where new ideas are most beneficial to introduce for better efficacy and in achieving the *purpose* of legislation. Currently emerging technologies are reproducing or even fortifying existing inequalities. When emerging

282 M. Ragnedda & G. Muschert, The Digital Divide: The Internet and Social Inequality in International Perspective, 18, 57, 58, 59 (2013)

283 *See, e.g.,* Broadband Internet – The New Digital Divide? ITU. Available: www.itu.int/newsroom/media-kit/story8.html Accessed: 20.11.2014

284 S. Dutta, B. Osoria-Bilbao &B. Lanvin. (Eds.) The Global Information Technology Report. Rewards and Risks of Big Data (2014)

technologies are adopted and eGovernance embraced in some European countries, the adoption of the same technology and regulation in other countries that are not digitally literate or skilled to the same extent might create privacy risks simply due to lack of capabilities and interest. Hence based on the research on patents and underlying technologies the common conclusion is that the problems, such as digital divide, cannot be solved by providing "Internet für Alle".[285] The approach should be a coherent regulatory framework where relevant and connected fields are developed hand in hand taking the context into account. This can be achieved by introducing a Car Pool Lane approach where several goals from different fields of law, or from different disciplines such as business and law are achieved by operating in close interaction and proceeding hand in hand in a balanced way laying ground for the next development step.

To crystallize the recommendation, in order to maximize the positive impacts and create spillover effects of ICT in the European Union, it must be understood that difference between member states in adopting eTechnologies or in protecting ePrivacy does not rise from the legislation or technology, but from combination of several aspects such as social and economic landscape. This is the problem with current regulatory framework also which Car Pool Lane approach intends to solve.

Finally, considering the current regulation, if the Car Pool Lane approach would have been introduced, there might have been a program for identifying for example how to finance and foster growth through Horizon 2020 in emerging technologies related to Big Data, whilst simultaneously assessing the means to respond to new ePrivacy concerns arising from these technologies. Implications would have been identified with multi-level impact assessment, and solutions might have been interdisciplinary solution: the Law being the foundation, and other means i.e. PETs complementing the purpose.

3. From Spider-Web to Safety Net

As is the case with spider webs, every web begins with a single thread, which forms the basis of

285 Popular slogan in the early 21st century and the name of German government's ten-point program "Internet für Alle – Schritte auf dem Weg in die Informationsgesellschaft" launched by Chancellor Gerhard Schröder in September 2000.

the next structure. To build a bridge between threads, spider releases new thread into the wind, and with luck, it catches onto another thread and so on. This can be seen to describe pretty accurately current European regulatory framework for ICT on ePrivacy. Certainly regulation is very advanced, but what is the ultimate purpose? To catch the subject?

Objectives of regulatory framework of ICT are not achieved by spider web-like regulation where the subjects are trapped in spider web having no clue what to do. First step is to remove the red tape unnecessary for the purpose of achieving the objectives. This conclusion can be made based on analysis limited to ePrivacy regulation in ICT, but it can be seen to be scalable to concern the European regulatory framework as a whole *inter alia* general objectives of the European Union such as sustainable development based on balanced economic growth and social justice and social inclusion.[286]

At first positivist approach should be limited.[287] Ultimately the goal is to secure the rights of the individuals such as right to privacy both in online and offline which means that also the ethical justification for the content of law should be taken into account. In a theoretical level safety net regulation means slightly leaning away from hierarchical and formal regulation.

One central aspect of suggested safety net regulation is the temporal aspect. Assessment should be made whether the regulation should be permanent or only for certain period of time. As an example, in intellectual property law the protection for the new invention is granted only for the limited period of time, due to fact that it is considered proportionate for only certain period i.e. necessary to promote technological advancements. Other aspect can be borrowed from competition law, whether regulation is reasonable i.e. the effects on relevant market are considered.

It might sound naive, but as my mentor and supervisor tend to say “with proportionality you never go wrong”. It applies also to European legislation, not only to the subjects to the legislation. The recommendation is that although spider-web is very advanced, it might not fully

286*See* Art. 3 of the Treaty of European Union

287Regulators as technicians of the law and jurists serving it literally uninterested in what is the purpose or objective. For consideration on the evolution of the European regulatory framework in ICT and the solutions to go forward, *see* J. Bauer, *The Evolution of the European Regulatory Framework for Electronic Communications*. IBEI Working Papers 2013/41 (2013)

serve the purpose, hence safety-net like EU regulation should be created.[288]

The term safety net also implies the role of legislation in protecting most fundamental rights by safeguards. Recommendation includes the assumption that 'internet' as an information and communication network is the foundation of much of critical infrastructure and will evolve to be a critical infrastructure superseding many specialized systems providing number of critical applications such as high data protection and privacy requiring tasks *inter alia* financial data transactions, eGovernance services such as eVoting and other security operations.[289] For these reasons, looking into future, the coherent regulatory framework for ePrivacy in ICT is essential which include both substantially intrusive regulations and directives without too much red tape, but also *sui generis* regulation and possibility to adopt case and context specific regulation.

Finally, in addition to recommendations and conclusions made, based on discussions on internet as a CI in the future, introducing new 'regulation on network and information security' as fast as possible is an important step and should be made by Commission considering the expanding role of internet and significance of Critical Information Infrastructure Protection (CIIP).[290] One of the most important aspects of the Directive, or preferably Regulation, would be asking member states to support the standardization process in the area of Network and Information Security (NIS).[291]

---

288 For two examples on regulation which had the potential to serve the purpose, but were introduced in spider web like framework creating more complex and ineffective regulation, *see* appendix 3.

289 For more information on future of Critical Infrastructure, cross-sectoral approach, international cooperation, privacy and information sharing between public and private sector, *see, e.g., European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security.* (2012) Available: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2012-237 Accessed: 20.12.2014

290 *See, e.g.,* 'Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union' Available: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security Accessed: 25.12.2014

291 M. Hathway, Best Practices in Computer Network Defense: Incident Detection and Response, 102 (2013)

III. Final Words

ePrivacy protection in the European regulatory framework can be considered to be very advanced regardless of what view one has on specific legal developments. The objective of the thesis was to identify possible problems and challenges in the European regulatory framework. Patents proved to be a useful source of data if used in a way contributing to a specified objective. In the same way EU law should be constantly developed, sometimes with inventive methods to contribute in achieving the initial purpose.

Although identifying possible problems based on patent information appears to be a negative approach by nature, it should be made clear that the European regulatory framework is the most advanced internationally providing unarguably the best protection of rights to privacy for individuals in digital world. Yet, one specific concern that remains is the extending responsibilities and obligations for the data controllers. It is the main field of concern in the future unarguably. Although the approach taken by CJEU and Commission can be seen to mitigate some risks, it can simultaneously create new risks to ePrivacy rights *inter alia* due to the fact that it is intended to concern also controllers that have only vague connections to Europe and concerns controllers in all levels such as engineers building IT systems. It is inevitable that the regulation is circumvened introducing new threats even more challenging to identify, not to mention regulate. If it is necessary to take further action, for example competition law should be introduced and regulatory measures and their impacts assessed not only during the drafting process, but also after the adoption. In case search engine operators are considered, dividing the search engine operations from other business operations and limiting the use of sensitive personal data vertically as well as over time can prove to be a rather effective measure.[292] This also directly mitigates the central problems in future ePrivacy protection which is not necessarily the collection, but the processing and future use of the data.

Technology is always faster than legal mind. Yet, law as 'slow' can be seen as a positive feature because law creates stability.[293] Understanding this helps to benefit from the best features of law and technology. However it does not mean that lawyers should fully understand the technology

292 Lawyers with knowledge on different fields of law or interdisciplinary knowledge surely can elaborate on the idea to come up with more advanced options.

293 Argument that law cannot keep up the pace of technology is relatively unproductive and irrelevant.

or engineers the law, merely to understand that technology can help in achieving the goals of law, and law can act as an enabler for technological development and steer it into most beneficial direction considering all the interest groups. For rights to exists in practice, obligations necessarily exist.[294]

The law is generally referred to when something is wrong. Hence we should be humbled by the fact that fundamentally the law is by the society and for the society covering the needs of Master Student in Law and Technology in Tallinn University of Technology as well as the ones of good-old farmer in rural areas of Romania.

I once heard the saying 'God gave us the Land and the Rights, EU stifled them'. I am confident that this view reflected the past Europe, and in the future regulation is the backbone for not equal but equitable Europe where uniqueness is taken into account. EU does not have to act like God giving land and rights, but the role is merely to protect them wisely.

294 Fundamental rights can be considered unconditional and universal applicable to all. Negative rights such as 'to be left alone' obliges others not to act against the right.

Bibliography

Books and Research Papers

Albers, M. Realizing the Complexity of Data Protection in Gutwirth, S., Leenes, R. & De Hert, P (Eds.) Reloading Data Protection Multidisciplinary Insights and Contemporary Challenges. Springer, Dordrecht (2014)

Bauer, J. The Evolution of the European Regulatory Framework for Electronic Communications. IBEI Working Papers 2013/41, Telefonica Chair Series. IBEI, Barcelona (2013)

Bowling, B., Marks, A. & Murphy, C. Crime Control Technologies: Towards an Analytical Framework and Research Agenda *in* Brownsword, R. & Yeung, K. (Eds.) Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes. Hart Publishing, Oxford (2008)

Coliver, S., Boyle, K., & F. D'Souza, F. Striking a Balance. Hate Speech, Freedom of Expression and Non-Discrimination. Article 19, London (1992)

Cooley, T. A Treatise on the Law of Torts. Or the Wrongs which Arise Independently of Contract. Callaghan & Company, Chicago (1906)

European Scrutiny Committee, House of Commons, Eleventh Report of Session 2012-2013. The Stationery Office, London (2012)

Fuster, G. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer Cham, Heidelberg (2014)

Giddens, A. The consequences of modernity. Stanford University Press, Stanford (1990)

Given, L. The Sage encyclopedia of qualitative research methods. SAGE Publications, Thousand Oaks (2008)

Grewlich, K. Governance in Cyberspace. Access & Public Interest in Global Communications. Kluwer Law International, The Hague (1999)

Gutwirth, S., Leenes, R. & De Hert, P. (Eds.) European Data Protection: Coming of Age, Springer, Dordrecht (2013)

Gürses, S. Multilateral Privacy Requirements Analysis in Online Social Networks. PhD thesis, KU Leuven (2010)

Hathway, M. Best Practices in Computer Network Defense: Incident Detection and Response. IOS Press, Amsterdam (2013)

Kerikmäe, T. (Ed.) Regulating eTechnologies In the European Union: Normative Realities and Trends. Springer Verlag, Heidelberg (2014)

Kokott, J. & Sobotta, C. The Charter of Fundamental Rights of the European Union after Lisbon. European University Institute, Academy of European Law, Fiesole (2010)

Kosta, E. Consent in European Data Protection Law. BRILL Academic Publishers, Leiden (2013)

Lawrence, J. A Catalog of Special Plane Curves. Dover Publications, New York (1972)

Leenes, R., Schallaböck, J. & Hansen, M. PRIME white paper, Privacy and Identity Management for Europe. PRIME (2008)

Lessig, L. Code and other laws of cyberspace. Basic Books, New York (1999)

Lloyd, I. Information Technology Law. Oxford University Press, New York (2011)

Madejski, M., Johnson, M. & M. Bellovin, The Failure of Online Social Network Privacy Settings. Columbia University Computer Science Technical Reports (2011)

Manolescu, D. Data Protection Enforcement: The European Experience – Case Law in Ismail, N. & Yong Cieh, E. (Eds.) Beyond Data Protection. Strategic Case Studies and Practical Guidance. Springer Verlag, Heidelberg (2013)

Montesquieu, C. De l'Esprit des Lois. Nourse, London (1772)

Moses, L. Sui Generis Rules in G. Marchant, B. Allenby & J. Heckert (Eds.), The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem. Springer, Dordrecht (2011)

Niemelä, M. & Pitkänen, O. Privacy and data protection in Emerging RFID-Applications. EU RFID Forum (2007)

Nissenbaum, H. Privacy In Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, Stanford (2010)

Pearson, S. & Benameur, A. Privacy, security and trust issues arising from cloud computing, Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010. IEEE Press (2010)

Perry, S. & Roda, C. Teaching Privacy by Design to Non-technical Audiences in Cleary, F. & Felici, M. Cyber Security and Privacy: Third Cyber Security and Privacy EU Forum, CSP Forum 2014, Athens, Greece, May 21-22, 2014, Revised Selected Papers. Springer, Heidelberg (2014)

Plato, Euthyphro, Apology, Crito, Phaedo, Phaedrus. Harvard University Press, Cambridge (1914)

Ragnedda, M. & Muschert, G. The Digital Divide: The Internet and Social Inequality in International Perspective. Routledge, New York (2013)

Rogers, M. The Definition and Measurement of Innovation. Melbourne Institute of Applied Economic and Social Research, Melbourne (1998)

Rull, A., Täks, E. & Norta, A. Towards Software-Agent Enhanced Privacy Protection, in Protection in Kerikäe, T. (Ed.), Regulating eTechnologies in the European Union. Springer Verlag, Heidelberg (2014)

Sheth, A. & Thirunarayan, K. Semantics Empowered Web 3.0 Managing Enterprise, Social, Sensor, and Cloud-based Data and Services for Advanced Applications. Morgan & Claypool Publishers, San Rafael (2013)

Solís, D. La Protección Judicial de los Derechos en Internet en la Jurisprudencia Europea. Editorial Reus, Madrid (2014)

Solove, D. Understanding Privacy. Harvard University Press, Cambridge (2008)

Solowe, D., Rotenberg, M. & Schwarz, P. Privacy, Information and Technology. Aspen Publishers, New York (2006)

Täks, E. & Lohk, A. An alternative method for computerized legal text restructuring, Proceedings of the 2010 conference on Legal Knowledge and Information Systems: JURIX 2010: The Twenty-Third Annual Conference. IOS Press, Amsterdam (2010)

Van Eecke *et al*. Legal analysis of a Single Market for the Information Society (SMART 2007/0037) (2009)

Weber, M. The Protestant Ethic and the Spirit of Capitalism. George Allen & Unwin, London (1930)

Walden, I. Telecommunications Law and Regulation. Oxford University Press, Oxford (2012)

Wong, R. Data Security Breaches and Privacy in Europe. Springer, London (2013)

Yar, M. Public perceptions and public opinion about Internet crime in Jewkes, Y. & Yar, M. (Eds.) Handbook of Internet Crime. Routledge, New York (2011)

Zervaki, A. Resetting the Political Culture Agenda: From Polis to International Organization. Springer Briefs in Law. Springer Cham, Heidelberg (2014)

Journals

Adrian, A. Has a Digital Civil Society Evolved Enough to Protect Privacy, 37 Alt.LJ 183 (2012)

Austin, L. Privacy and the Question of Technology, 22 Law and Philosophy 119 (2003)

Barney, A. & Jonathan, A. Study of Patent Mortality Rates: Using Statistical Survival Analysis to Rate and Value Patent Assets, 30 AIPLA Quarterly Journal 319 (2002)

Berring, R. Legal Research and the World of Thinkable Thoughts, 2 J. App. Prac. & Process 305 (2000)

Changwoo, C., Seungkyum, K. & Yongtae, P. A patent-based cross impact analysis for quantitative estimation of technological impact: The case of information and communication technology, 74 TECHNOL FORECAST SOC 1296 (2007)

Cockfield, A. Transforming the Internet into a Taxable Forum: A Case Study in E-Commerce Taxation, 85 Minn. L. Rev 1171 (2001)

Coglianese, C. Information Technology and Regulatory Policy: New Directions for Digital Government Research, 22 SSCR 85 (2004)

Diggelmann, O. & Cleis, M. How the Right to Privacy Became a Human Right, 14 Human Rights Law Review 441 (2014)

Frame, J. & Tong, X. Measuring national technological performance with patent claims data, 23 Res Policy 133 (1994)

Fujii, A. Iwayama, M. & Kando, N. Introduction to the special issue on patent processing, 43 Inform Process Manag 1149 (2007)

Gavison, R. Privacy and the Limits of Law, 89 Yale L.J. 471 (1980)

Hiselius, P. ICT/Internet and the right to Privacy, 56 Scandinavian Stud. L. 201 (2010)

Kerper, J. Creative Problem Solving vs. the Case Method: A Marvelous Adventure in which Winnie-the-Pooh Meets Mrs. Palsgraf, 43 Cal. W. L. Rev 351 (1998)

Kokott, J. & Sobotta, C. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, 3 IDPL 222 (2013)

Koops, B-J. & Leenes, R. Privacy regulation cannot be hardcored. A critical comment on the 'Privacy by design' provision in data-protection law, 28 IJLIT 159 (2014

Kwecka, Z. et al. ‘‘I am Spartacus’’: privacy enhancing technologies, collaborative obfuscation and privacy as a public good, 22 Artiff Intell Law 113 (2014)

Marshoof, A. Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression, 19 Int J Law Info Tech 110 (2011)

Narin, F. Patent bibliometrics, 30 Scientometrics 144 (1994)

Nissenbaum, H. Toward a Approach to Privacy in Public: Challenges of Information Technology, 7 Ethics Behav 207 (1997)

Nyman-Metcalf, K. & Täks, E. Simplifying the law—can ICT help us?, 21 Int J Law Info Tech 239 (2013)

Prins, C. Biometric technology law, Making our body identify for us: Legal implications of biometric technologies,14 CLSR 159 (1998)

Swire, P. & Lagos, Y. Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 Maryland Law Review 335 (2013)

Tribe, L. Technology Assessment and the Fourth Discontinuity: The Limits of Instrumental Rationality, 46 S. Cal. L. Rev 617, (1973)

Virtanen, P. Innoweb v Wegener: CJEU, sui generis database right and making available to the public – The war against the machines, 5 EJLT Commentaries (2014)

Warren, S. & Brandeis, L. The Right to Privacy, 4 Harv. L. Rev. 193 (1890)

Other Legal Sources

Albrecht, J. Brief of Amicus Curae Jan Philipp Albrecht on Microsoft Corporation v United States of America (2d Cir. 2014)

Article 29 Data Protection Working Party, Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism (2004)

Article 29 Data Protection Working Party, Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (2005)

Article 29 Data Protection Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR) (2007)

Article 29 Data Protection Working Party & Working Party on Police and Justice, 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 (2009)

Article 29 Data Protection Working Party, Advice paper on special categories of data ("sensitive data") (2011)

Article 29 Working Party Opinion, 04/2012 on Cookie Consent Exemption (2012)

Article 29 Data Protection Working Party, Adoption of guidelines on the implementation of the CJEU's Judgment on the "right to be forgotten" (2014a)

Article 29 Data Protection Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgement on 'Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/121(2014b)

Council of Europe, Parliamentary Assembly resolution 1843. The protection of privacy and personal data on the internet and online media (2011)

Council of the European Union, Main results of the Council, 3354th Council meeting Justice and Home Affairs (2014)

Court of Justice of the European Union, The Court of Justice declares the Data Retention Directive to be invalid (2014)

Dutta, S. Osoria-Bilbao, B. & Lanvin, B. (Eds.) The Global Information Technology Report. Rewards and Risks of Big Data. World Economic Forum (2014)

European Commission, European Commission swears oath to respect the EU Treaties (2010)

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Safeguarding Privacy in a Connected World a European Data Protection Framework for the 21st century (2012)

European Commission, European Commission and data industry launch €2.5 billion partnership to master Big Data (2014)

European Commission, Eurostat regional yearbook 2014. Eurostat statistical books (2014)

European Commission, Factsheet on the "Right to be Forgotten" Ruling (C-131/12) (2014)

European Commission, Progress on EU data protection reform now irreversible following European Parliament vote, Memo14/186 (2014)

European Commission of Human Rights, Council of Europe, Preparatory Work on Article 8 of the European Convention on Human Rights (1956)

European Data Protection Supervisor, EDPS letter to the Council of Ministers regarding progress on the data protection reform package (2014)

European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law (2014)

High Level Group on Administrative Burdens, Cutting Red Tape in Europe (2014)

Hustinx, P. EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation (2014)

Hustinx, P. The moment of truth for the Data Retention Directive, Conference 'Taking on the Data Retention Directive' (2010)

Kroes, N. eID: unlocking confidence and convenience in a Digital Single Market. The eIDAS Regulation Launching Event Brussels, 14 October 2014

Nyman-Metcalf, K. Lectures in Legal Framework of e-governance. Tallinn University of Technology (2014)

OECD, Guide to Measuring the Information Society 2011 (2011)

Appendices

Appendix 1. ICT fields According to IPC Classes.

ICT fields According to IPC Classes

• Telecommunications:
G01S,G08C,G09C,H01P,H01Q,H01S3/
(025,043,063,067,085,0933,0941,103,133,18,19,25),
H1S5,H03B,H03C,H03D, H03H,H03M,H04B,H04J,H04K,H04L,H04M and H04Q

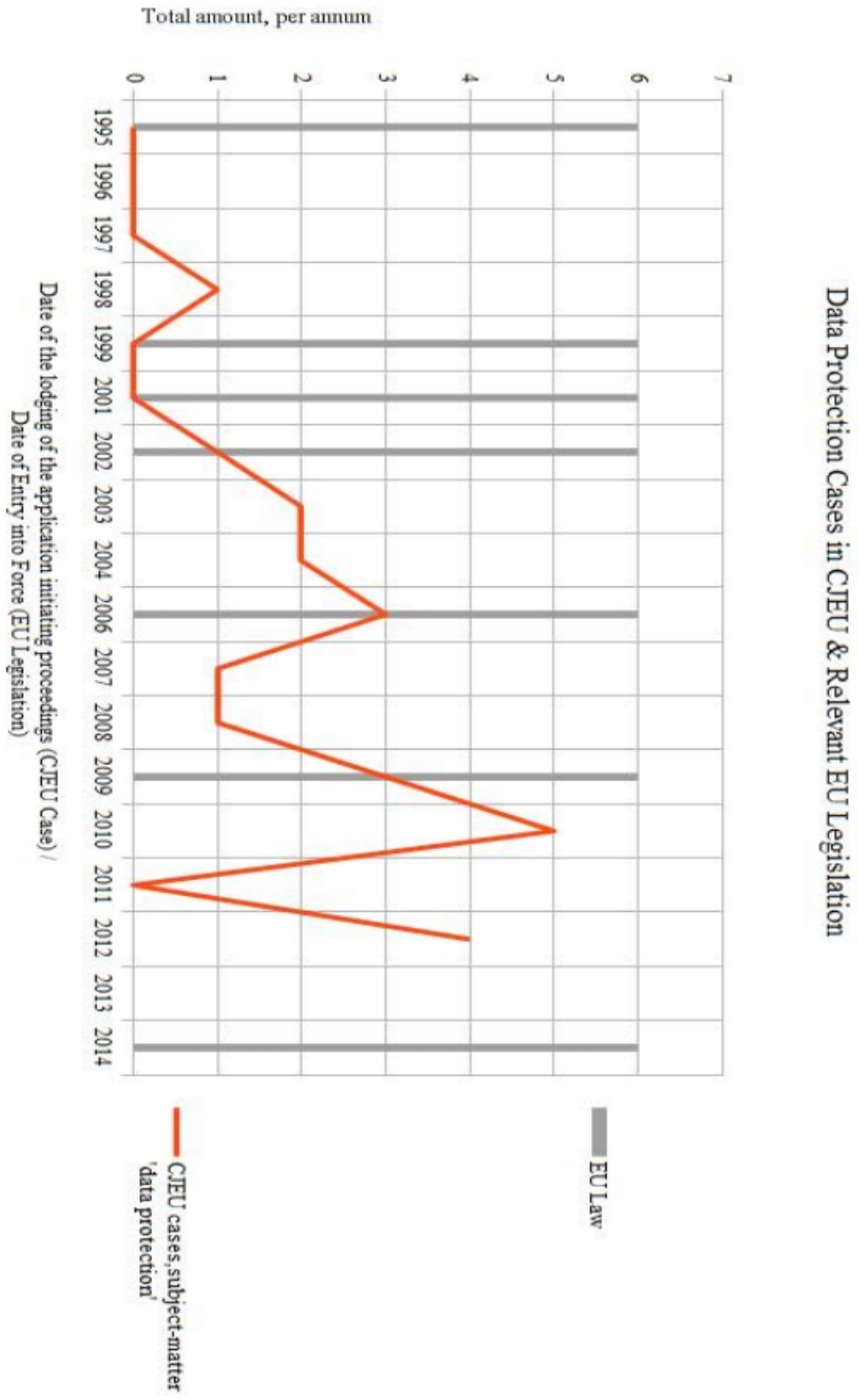
• Consumer electronics:
G11B,H03F,H03G,H03J,H04H,H04N,H04R and H04S

• Computers, office machinery:
B07C,B41J,B41K,G02F,G03G,G05F,G06,G07,G09G,G10L,G11C,H03K and H03L.

• Other ICT:
G01B,G01C,G01D,G01F,G01G,G01H,G01J,G01K,G01L,G01M,G01N,G01P,G01R,G01V,
G01W,G02B6,G05B,G08G,G09B,H01B11,H01J(11/,13/,15/,17/,19/,21/,23/,25/,27/,29/,31/,
33/,40/,41/,43/,45/) and H01L.

ICT fields according to IPC classes. Source: OECD (2011)

Appendix 2. Data Protection Cases in CJEU & Relevant EU Legislation



Appendix 3. From Spider-Web to Safety Net

Thinking. Out. Loud. – project 2015

Tommi Sundqvist

Pro Mercatoria L.A.B.

DRAFT

"Democracy must be built through open societies that share information. When there is information, there is enlightenment. When there is debate, there are solutions. When there is no sharing of power, no rule of law, no accountability, there is abuse, corruption, subjugation and indignation."

- Atifete Jahjaga

From Spider-Web to Safety Net

As is the case with spider webs, every web begins with a single thread, which forms the basis of the next structure. To build a bridge between threads, spider releases new thread into the wind, and with luck, it catches onto another thread and so on. This can be seen to describe pretty accurately current European regulatory framework for ICT on ePrivacy. Certainly regulation is very advanced, but what is the ultimate purpose? To catch the subject?

Although spider web is very advanced, it might not fully serve the purpose, hence safety-net like ICT law should be created for EU. The term 'safety net' implies the role of regulation in protecting most fundamental rights by safeguards, not by prohibitive law.

At first (Germanic) ultra-positivist approach should be abandoned.[1] Ultimately the goal is to secure the rights of the individuals such as right to privacy both in online and offline, not to regulate black different from white. In a theoretical level this means slightly leaning away from hierarchical and formal regulation, whereas in practical level it means the introduction of positive norms.

One central aspect of safety net regulation is the temporal aspect. Assessment should be made whether the regulation should be permanent or only for certain period of time. As an example, in Intellectual Property law the protection for the new invention is granted only for the limited period of time, due to fact that it is considered proportionate for only certain period i.e. necessary to achieve the protection to promote technological advancements. Other aspect can be borrowed form competition law, the effect, whether regulation is reasonable i.e. the effects on market are considered.

1 For consideration on the evolution of the European regulatory framework in ICT and the solutions to go forward, see Bauer, J. The Evolution of the European Regulatory Framework for Electronic Communications. IBEI Working Papers 2013/41. Telefonica Chair Series. 2013

The balance of ex ante and ex post regulation is also significant in transformation from spider web regulation to safety net regulation. It is important to note that, although the Court is keen to stress that the ex ante and ex post regimes are distinct rules which serve different purposes, in practice they are connected. For example in the Telefónica Case 398/07, Kingdom of Spain v Commission, [2012] , where Telefónica was former state owned monopoly telecommunication provider providing both wholesale products as well as retail products, was found abusing dominant position by Court. The reason Telefónica was offering wholesale products was because it was obliged to do so by national ex ante regulation. In other words, it breached ex post competition law by complying with its ex ante obligations.

Two examples on regulation can be given which had the potential to serve the purpose, but were introduced in spider web like regulatory framework creating more complex and ineffective regulation. It was claimed that 'technical implementing measures' in Regulation 611/2013 clarifies and confirms the measures which telecommunications operators, internet service providers and other providers of publicly available electronic communications services are required to take if their customers' personal data is lost, stolen or otherwise compromised. Article 2 of the Directive stipulates that the provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible, and the information included are set out in Annex I inter alia date and time of incident; circumstances of the personal data breach e.g. loss, theft, copying; nature and content of the data; technical and organizational measures taken; and possible cross border issues. Article 3 provides that when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, provider shall notify the subscriber or individual of the breach. It certainly can be argued that these requirements are very specific and clearly stated, but it certainly does not mean that it creates clarity on regulatory framework.

Second example is the now void Data Retention Directive 2006/24/EC, which provided in Article 5 of the Directive categories to be retained inter alia data necessary to trace and identify the source of a communication; data necessary to identify the destination of a communication; data necessary to identify the date, time and duration of a communication; data necessary to identify the type of communication; data necessary to identify the location of mobile communication equipment; and data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained. These requirements do not either look like safety net, but spider web.

Although, moving towards safety net, it does not mean that sui generis regulation or data protection regulation including sanctions or monetary penalties should be abandoned. Quite contrary. The safety net does not mean removing all the obligations and prohibitions, but using them efficiently, which means using proportionate measures considering the context.

New developments create new ePrivacy related concerns in ICT almost on a daily basis such as 'converged content' where content is partially provided by individuals and partially by businesses. The regulation should be flexible enough to effectively respond to the threats to the privacy risks related to the sharing of data and creating content where the ownership of data is not clear, or private information or personal data is made public.[2]

2 *See* clipgenerator (*http://www.clipgenerator.com/*) for converged content i.e. movie clip consisting of personal messages, multimedia and desirable pop chart music which can be made public and shared.