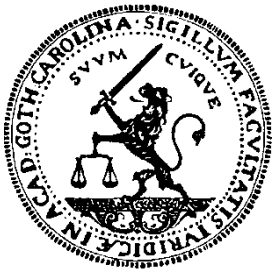

FACULTY OF LAW
Lund University

Elena Izyumenko

Think before you share: Personal data on the Social Networking Sites in Europe; Article 8 ECHR as a tool of privacy protection

Master thesis
30 credits

Supervisor: Ulf Maunsbach

Master´s Programme in International Human Rights Law and Intellectual Property Law

Spring 2011

Contents

Summary

The current research aims to find out how the European legal system may approach the challenges of the online social networking and their effects on the right to privacy in personal data protection of the European users. Since the answer closely depends on the nature of the right in question (human right or property right), the thesis involves a comparative analysis of the American and European privacy models. Ruling on the human rights nature of personal data protection in Europe, as well as on the correspondent privacy abusing practices of the online social networking business on the European ground, the examination further concentrates on the Article 8 ECHR possibilities to protect the right to privacy in personal data. The analysis of the ECHR case law will lead to conclude on the matter of existence of positive obligations of the States parties to the Convention to ensure an effective enjoyment of the right to privacy of the European users of the SNSs, in a sense of a recognition of an indirect horizontal effect of the Convention's provisions on the relationships between the users of the services, from one hand, and the social networking companies, providing their services in Europe, - on the other (irrespective of the territories of the countries from which such services are provided – be they within the European borders, or, as is the case with Facebook and other the most popular social networking platforms, - within the borders of the USA).

At the European level, the Council of Europe's Member States are under a positive obligation to act in a proactive manner with a view to securing the effective enjoyment of protected rights. The failure to do so may render a State liable under the ECHR, if it can be established that the State has failed to take appropriate measures within its power to protect the individuals under its jurisdiction from the right to privacy violations on the part of, *inter alia*, American social networking companies.

Thus, when considering the emerging trends in online social networking and in anticipation of potential (as well as of already existing) human rights violations in connection with its use, the Council of Europe Member States need to prepare themselves to deal with situations related to Article 8 with regard to the practices of treating the other people's personal data by online business.

Preface

I would like to thank my supervisor, Ulf Maunsbach, my wonderful family and amazing friends. Without your support, help and advice, the current work would never have been completed. I am grateful as well to all of the staff of the Law Faculty of Lund University who make a learning process there a real pleasure. I would also like to thank all of my my classmates: your intelligence and the true belief in Human Rights have served as an inspiration for me during the whole course of this Master Programme and while conducting the current research in particular.

Abbreviations

App	Application software
CEO	Chief Executive Officer
COE	Council of Europe
EC	European Community
ECC	European Convention on Cybercrime
ECHR	the European Convention on Human Rights
ECtHR	the European Court of Human Rights
EEC	European Economic Community
EPIC	Electronic Privacy Information Center
EU	European Union
IP address	Internet Protocol address
ISP	Internet Service Provider
OECD	Organisation for Economic Cooperation and Development
PIPEDA	Personal Information Protection and Electronic Documents Act
SNS	Social Networking Site

Introduction

The current research focuses on the human rights possibilities of personal data protection in Europe, needed to face the challenges of a newly developing digital technologies, with the phenomenon of online social networking being at the core of this process. The preliminary answer to these challenges, as well as a foundation of the possibilities of protection, is argued to be found in Article 8 of the ECHR and the respective case law of the Strasbourg Court.

The interest in the issue is well-timed given a still extremely "young age" of the social networking sites (SNSs), as well as the recent tendencies of the ECHR case law towards developing the ideas of positive obligations of the State parties, indirect horizontal application of the Convention rights, taken together with transjurisdictional implications of online activities.

As to the methods used while conducting the current research, they are mainly the following: 1) the qualitative evaluation of the primary and secondary sources touching upon the problem at issue, as well as 2) the comparative analysis, involving the two major systems of personal data protection, namely – the one existing in the USA, and the other developed on the European ground.

The argumentation will be structured as follows.

Chapter 1 will give an explanatory background as to the nature of online social networking, through the prism of its role in pushing the boundaries of the modern privacy landscape. The respective subchapters will go into analyzing, in particular: the claimed modern understandings of privacy as of "a new social norm" (subchapter 1.1.); the shifts in the main actors models on the arena of personal privacy from the "State v. individual" towards "private business v. individual" relations (subchapter 1.2.); the tendencies towards commodification of personal information (subchapter 1.3.); finally, the analysis will go briefly into the origins of information privacy violations, which are viewed as being indirectly initiated by the users of the online social networking services themselves (subchapter 1.4.).

Chapters 2 and 3 will focus on the theoretical debate around the meaning of the right to privacy in general and information privacy in particular (Chapter 2), followed by a review of the relevant European legislation, as well as of its historical development (Chapter 3).

Moving further, Chapter 4 will be devoted to analyzing of the two main worldwide privacy models. The named analysis will prove to be of a crucial importance for the whole line of argumentation of the current research, as the legal outcomes and conclusions are directly dependant on the choice of a particular model. Thus, the first part of the instant chapter will go into a

comparative examination of an American model, treating information privacy as a commodity or a property right (subchapter 4.1.), and European model, seeing the data privacy as an integral part of a more broad in its scope right to privacy, and, consequently, as a human right (subchapter 4.2.). The second part of the promised analysis will go to provide some counterarguments of those, claiming that even on the European ground there is a floor for a proprietary treatment of personal data (subchapter 4.3.). In response to such claims the closing subchapter (4.4.) will clarify the necessity to concentrate (in the current legal analysis) on the actual legal rules in practice, rather than on philosophical debates, arguing, subsequently, that the relevant European law and specifically Article 8 ECHR case law serve as a profound evidence of a human rights nature of the right to personal data protection in Europe. Being of a human rights nature, it will be argued, such right cannot be contracted around freely on the basis of a contractual agreement – it cannot be waived or sold in exchange for the social networking services.

Having reached the conclusion on the human rights nature of the right to privacy in personal data in Europe, Chapter 5 will aim to demonstrate that the modern online social networking practices impose real and profound dangers to the right to privacy of their users. Moreover, these dangers, taken cumulatively, having reached such a high scale, on which the violation of the human right to privacy in data protection can be (and should be), in fact, claimed. In order to fulfill the announced aim, first, the basic principles of personal data protection on the European ground are analysed (subchapter 5.1.) with the purpose, second, to trace their implications on the SNSs (subchapter 5.2.). The latter is done through the prism of examination of specific challenges that online social networking business brings with it, such as, *inter alia*, confusing privacy policies, privacy-abusing ways of collection, sharing and rectifying of personal information, and etc.

Finally, as a response to the right to privacy violations proved to exist and flourish in the realm of online social networking, Chapter 6 will address the question of how to protect the right to privacy in personal data of the European users. The solution will be demonstrated to be inherent in Article 8 ECHR. As a part of the instant analysis, the four lines of the Strasbourg Court's case law will be examined. The conclusion is to be reached on the matter of existence of positive obligations of the State parties to the ECHR to ensure an effective enjoyment and protection of the right to privacy of the individuals within their jurisdictions from the violations on the part of the non-European (primarily American) social networking companies.

1 Social networking and the changing privacy landscape

Having deservedly gained the name of "one of the most successful stories in the life of the Internet",[1] online social networking in a very short period became a mainstream cultural phenomenon and one of the most popular activities on the web.[2] A huge phenomenon as such, social networks are also a part of the broader process of the growth and innovation in the information technology sector.[3] From even a more broad perspective they are indispensible part of globalization with all its positive and negative consequences.

Though rapidly evolving, social networks are still extremely "young".[4] Not more than seven years ago Facebook didn't exist, and Googling wasn't yet a verb.[5]

The pace with which social networking is evolving is staggeringly unprecedented. As Paul Virilio has emphasised, new technologies always bring about even more and even faster new technologies.[6] Since 2004 (the year when it was founded) Facebook has grown from a mere college site, conceived in a Harvard dorm, to a huge corporation embracing more than half a billion users.[7] Yet it already became the largest of the social

---

[1] M Kacimi, S Ortolani & B Crispo, 'Anonymous Opinion Exchange over Untrusted Social Networks', *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*, Nuremberg, Germany, March 31, 2009, p. 26, <http://www.inf.unibz.it/~mkacimi/eurosys2009.pdf>.

[2] J Bonneau & S Preibusch, 'The Privacy Jungle: On the Market for Data Protection in Social Networks', *The Eighth Workshop on the Economics of Information Security*, WEIS, 2009, p. 4 <http://preibusch.de/publications/Bonneau_Preibusch__Privacy_Jungle__2009-05-26.pdf>.

[3] P Swire, 'Social Networks, Privacy, and Freedom of Association. How Individual Rights Can Both Encourage and Reduce Uses of Personal Information', *Center for American Progress*, February 2011, p. 6, <http://ftc.gov/os/comments/privacyreportframework/00342-57843.pdf>.

[4] ibid., p. 9.

[5] J Stoddart, 'The Path to Proactive Privacy. Remarks at the 1st Annual Privacy and Information Security Congress 2010 organized by Reboot Communications Ltd.', in *Office of the Privacy Commissioner of Canada*. Ottawa, Ontario, November 15, 2010, <http://www.priv.gc.ca/speech/2010/sp-d_20101115_e.cfm>.

[6] P Virilio, *Die Eroberung des Körpers: Vom Übermenschen zum überreizten Menschen*, München, Wien, 1994, cited in M Friedewald, 'A New Concept for Privacy in the Light of Emerging Sciences and Technologies', *From the SelectedWorks of Michael Friedewald*, April 2010, p. 72, <http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=michael_friedewald>.

[7] Swire, *Center for American Progress*, p. 9.

networking sites.[8]

Other web sites of the kind have undergone a similar explosive growth. YouTube was launched just a year after Facebook - in 2005, and by now the company claims around 24 hours of new videos being uploaded each minute.[9] One year later (in 2006) Twitter was introduced and currently is estimated as having more than 200 million active users, posting around 65 million tweets a day.[10]

The amount of digital information that was created only in 2010 in blogs, tweets and social networks is estimated in 1.2 zettabytes – an equivalent to a television series being broadcasted continuously (and without commercials) for 125 million years.[11]

The voluntary sharing of personal information on such a scale represents a dramatic shift in social mores and behaviour,[12] making the world a smaller place, a so-called "global village". The fact that all of this personal information is stored somewhere, can be easily used and equally easily abused[13] triggers new challenges to the free exercise of human rights and fundamental freedoms, the long-term consequences of which are only starting to be considered and studied.[14]

The SNSs enable observation, storage and analysis of the most day-to-day human activities, more easily, rapidly and invisibly than ever before, potentially creating a feeling of being permanently watched.[15] They represent "a modern form of surveillance" or, as some authors prefer to call it – "dataveillance".[16]

---

[8] J Stoddart, 'Privacy in the era of social networking: Legal obligations of social media sites. Remarks at the University of Saskatchewan College of Law Lecture Series', in *Office of the Privacy Commissioner of Canada*. Saskatoon, Saskatchewan, November 22, 2010, <http://www.priv.gc.ca/speech/2010/sp-d_20101122_e.cfm>.

[9] ibid.

[10] M Shiels, 'Twitter co-founder Jack Dorsey rejoins company', in *BBC News. Business*. 28 March 2011, viewed on 5 May 2011, <http://www.bbc.co.uk/news/business-12889048>.

[11] T Jagland, Secretary General of the Council of Europe, *Speech made on the Data Protection Day (30th Anniversary)*, Brussels, 28 January 2011, p. 10, <http://www.data-protection-day.net/files/Introduction_0_1_SG_Jagland_OK_FOR_WEBSITE_FINAL.pdf>.

[12] Stoddart, 'Privacy in the era of social networking'.

[13] Jagland, p. 11.

[14] C Bernier, 'Online Behavioral Advertising and Canada's Investigation on Facebook. Remarks at the Privacy Laws and Business 23rd Annual Conference', in *Office of the Privacy Commissioner of Canada*. Cambridge, United Kingdom, July 6, 2010, <http://www.priv.gc.ca/speech/2010/sp-d_20100706_cb_e.cfm>.

[15] Jagland, p. 12.

[16] D Zwick & N Dholakia, 'Models of Privacy in the Digital Age: Implications for Marketing and E-Commerce', *American University, University of Rhode Island*, September

A huge amount of personal data that is gathered about individuals, that is processed and shared, often without their knowledge, raises troubling questions about people's capacity to control their own identities, to live freely and in respect for their privacy.[17]

The outlined reasons have made social networking sites the front lines in the privacy protection battles all around the world.[18]

To sum up, we are in a rough time, with phenomenal burdens lying on information privacy. The challenges are profound, they're complex, and they're constantly evolving, while the consequences are not always predictable.[19] As the social networking continues to be a "cool new tool", we should stay connected to its emerging technologies, its social norms and market models, and – specifically - its legal and policy queries.[20]

The current chapter explores the most prominent shifts made by social networking in the information privacy landscape. The examination of these shifts is fundamental for the better understanding of the whole subsequent legal analysis. In short, these shifts are:

1) a changed nature of privacy, which the leaders of the social networking business vigorously promote in order to, in a sense, justify the next shift, –
2) shift from vertical to horizontal relations between the main actors on the arena of information privacy;
3) commodification of personal information;
4) violations are currently being indirectly initiated by the users themselves, as they voluntarily publish their data on the SNSs based on the assumed consent with the companies' privacy policies.

One more important feature that the SNSs have brought with them, though not examined in details under the current chapter, is – the transborder, global nature of the data flows that the SNSs permit. The phenomenon has important impact upon deciding on the matter of jurisdiction, and for this reason will be addressed later in the course of the current paper's legal analysis.[21]

7, 1999, p. 3, <http://ritim.cba.uri.edu/Working%20Papers/Privacy-Models-Paper%5B1%5D.pdf>.

[17] Stoddart, 'The Path to Proactive Privacy'.

[18] Stoddart, 'Privacy in the era of social networking'.

[19] Stoddart, 'The Path to Proactive Privacy'.

[20] T Mitrano, 'Facebook 2.0', *EDUCAUSE Review*, vol. 43, no. 2, March/April 2008, <http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume43/Facebook20/162687>.

[21] See Chapter 6, Subchapter 6.4.

1.1 "A new social norm"

Those standing behind the social networking business claim a shift in understanding of what privacy is in a modern society. In essence, they suggest that privacy is pretty much dead in this era of digital exhibitionism.[22]

Just a few, but rather indicative (and forever infamous in privacy circles) statements made by the leaders of the hugest social networking corporations are presented below.

In 1999, Scott McNealy, a co-founder of a computer technology company "Sun Microsystems", when asked about the impact of new products on the privacy of those using the new technology, said: "You have zero privacy anyway… Get over it."[23]

More recently the head of one of the giants of the online world – Google – Eric Schmidt, when asked on the matter of sensitive privacy-protective issues, operated with an old version of "nothing to hide, nothing to fear" argument. What he argued is that "if you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[24]

Facebook and its CEO Mark Zuckerberg have taken the position that sharing of information and connectedness is the new social norm, and that privacy in the light of it is outmoded.[25]

Such an approach has left Facebook, together with the other social networking companies, trying to innovate its way around a fundamental human right that such companies (and it will be proved further)[26] do have a responsibility to respect – privacy.[27]

It can be easily agreed that the concept of privacy is changing. That is nothing new – what privacy means to us has without any doubt been evolving since we lived in caves. Privacy looks different today than it did a

---

[22] J Stoddart, 'Why Privacy Still Matters in the Age of Google and Facebook and How Cooperation Can Get Us There. Remarks at the 2010 Access and Privacy Conference', in *Office of the Privacy Commissioner of Canada*. Edmonton, Alberta, June 10, 2010, <http://www.priv.gc.ca/speech/2010/sp-d_20100610_e.cfm>.

[23] C Docksey, 'EU Data Protection: The Development of a New Right of Privacy in Europe', Warsaw, 10 March, 2007, p. 1, <http://www.cels.law.cam.ac.uk/events/Docksey_30March.pdf>.

[24] Stoddart, 'Why Privacy Still Matters'.

[25] M Roggensack, 'Face It Facebook, You Just Don't Get It', in *Human Rights First*. May 25, 2010, viewed on 5 May 2011, <http://www.huffingtonpost.com/human-rights-first/face-it-facebook-you-just_b_589045.html>.

[26] See, *inter alia*, Chapter 4, Subchapter 4.4., and Chapter 6 of the current paper.

[27] Roggensack.

generation – or even a decade – ago.[28]

It doesn't exclude, though, the mere fact that privacy remains an incredibly important and cherished value for people around the world.[29] And of course it is not deprived of its fundamental human rights character.

The people exploiting the idea of privacy as of something outmoded are simply those who want to profit from its imaginable demise. These people are in the business of making money from the use of personal data – it's no wonder they would like everyone to think that privacy doesn't matter.[30] The pressure on information privacy is not the result of a new social norm. It comes from a desire to earn money at the expense of pushing the privacy protection boundaries.[31]

Such a role an online business plays in a changing technological and privacy landscape leads us to the next consideration within the theme of the current chapter, which is – the shift of privacy challenges from vertical (State v. individual) to horizontal (private business entities v. individual) relations.

1.2 From the "State v. individual" towards "private business v. individual" relations on the personal privacy landscape

The other fundamental challenge of the digital society in general and social networking in particular may be seen in the shift from vertical to horizontal relations between the main actors on the arena of personal privacy.

As Saskia Sassen has fairly pointed out, "suddenly, over the last few years, the two major actors in electronic space - the corporate sector and the civil society - which until recently had little to do with one another in electronic space, are running into each other."[32]

Governments are not any more the sole players on the stage of personal privacy. They are not even the main actors.[33]

---

[28] Stoddart, 'Why Privacy Still Matters'.

[29] ibid.

[30] ibid.

[31] ibid.

[32] S Sassen, *The Topoi of E-Space: Private and Public Cyberspace*, viewed on 6 May 2011, <http://fortunaty.net/com/textz/textz/sassen_saskia_the_topoi_of_e-space.txt>.

[33] Humanrightsfirst.org, 'Business And Human Rights', in *Human Rights First*, viewed on 5 May 2011, <http://www.humanrightsfirst.org/our-work/business-and-human-rights/>.

"Corporations have reached a level of influence that makes them both a problem and a potential solution in human rights struggles and requires a dual effort: holding them accountable for their actions (and the actions of their suppliers) while also providing a path so that their actions can support a positive human rights agenda".[34]

1.3 Commodification of personal information

The social networking has also created the trend of commodification of personal information.[35] It means the transformation of what is normally used to be a non-commodity into a commodity; in other words – assigning economic value to something that traditionally would not be considered in economic terms.[36] This is the case with personal data, which in the "new" economy have acquired an independent economic value, and consequently became the object of quasi-property rights making the information about individuals a tradable good.[37]

The incentives for the social networking companies to process personal data are high: information means money as well as power, while its collection by means of the SNSs is easy and cheap (due to the low-threshold facilities).[38]

Given profits personal information brings and costs its collection and processing require, marketers soon realized an opportunity to avoid the costs by buying the needed data from already existing databases of other enterprises.[39] Direct marketing business shows without any hesitation that personal data and profiles based on personal information are a booming source of income.[40]

---

[34] ibid.

[35] Stoddart, 'Privacy in the era of social networking'.

[36] B Hugenholtz, **'**Commodification of Information: The Future of the Public Domain', Amsterdam, January 2004, p. 1, <http://www.ivir.nl/agenda/iter/PapersCommodification/Final%20Background%20Paper1.doc>.

[37] Hugenholtz, p. 2.

[38] C Prins, 'Property and Privacy: European Perspectives and the Commodification of our Identity', *The future of the public domain*. Tilburg University, The Netherlands, 2006, p. 3.

[39] D J Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy', *Stanford Law Review*, 2001, No 53, p. 1407, cited in N Purtova, 'Property in Personal Data: a European Perspective on the Instrumentalist Theory of Propertisation', *European Journal of Legal Studies*, 2010, 2, 3, The Future of... Law & Technology in the Information Society, p. 3, <http://cadmus.eui.eu/bitstream/handle/1814/15124/10_Property_EN.pdf?sequence=1>.

[40] C Cuijpers, 'A Private Law Approach to Privacy; Mandatory Law Obliged?' *SCRIPTed*, vol. 4, issue 4, September 2007, p. 305.

Users of the social networking platforms react to these business practices in different ways (some find it chilling, others do not care at all).[41] And although some try to protect their privacy by applying techniques to 'hide' their data, actual and effective transparency and control remain unattainable. It is no longer possible for individuals to really find out what happens to their personal data, let alone that they are not in the position to effectively control the dealings with these data. Consequently, many individuals understandably try to gain as many benefits as possible from what is left of their privacy. To them, the only workable solution appears to be to 'sell' their personal information in exchange for the SNSs' services.[42]

1.4 Violations are indirectly initiated by the users themselves

Most of the personal information published on the SNSs appears there at the initiative of the users and based on their assumed consent.[43] In other words, the observation is initiated by the actions of its target him- or herself.[44]

As has been pointed out in the Report of the International Working Group on Data Protection in Telecommunications: "While "traditional" privacy regulation is concentrated on defining rules to protect citizens against unfair or unproportional processing of personal data by the public administration (including law enforcement and secret services), and businesses, there are only very few rules regulating the share of personal information at the initiative of private users, partly because this had not been a major issue in the "offline world", and neither on the Internet before the SNSs came into being. Furthermore, the privilege in data protection and privacy legislation had been given traditionally to the processing of personal data from the public sources."[45]

***

Concluding the above observation, it is important to note the following before we proceed further: the current paper will argue and will try to prove that social networks as such are not incompatible with personal data privacy, the fundamental principle of which is that an individual should have control

---

[41] Lundblad argues that we live in a 'noise society', characterized by a high collective expectation of privacy, but a low individual expectation of privacy. N Lundblad, 'Privacy in a Noise Society', *St Anna Institute*, Stockholm, 2004, <http://www.sics.se/privacy/wholes2004/papers/lundblad.pdf>.

[42] Prins, p. 7.

[43] International Working Group on Data Protection in Telecommunications, *Report and Guidance on Privacy in Social Network Services. "Rome Memorandum"*, 43rd meeting, 3-4 March 2008, Rome (Italy), p. 1.

[44] Zwick & Dholakia, p. 6.

[45] *Report and Guidance on Privacy in Social Network Services*, p. 1.

over how his or her personal data are used.[46] Any incompatibility is between those principles and the desire (as demonstrated in the statements of the leaders of social networking business) of those who run some of these networks to sell their users' information to other companies.[47]

It can't be denied that the phenomenon of social networking has forced us to more closely examine and redefine our understanding of privacy,[48] not undermining though its value, importance and its place in the row of basic human rights.

Therefore, it is logical to start the analysis with setting the frameworks for how the privacy (with a particular attention to information privacy) may be defined, followed by the description of legislative origins and historical development of the concept in Europe, along with its modern meaning.

[46] The principle of control, together with some other basic principles of personal data protection is examined more closely in Chapter 5.

[47] Tavenerslaw.co.uk, 'Are social networks and European data privacy laws incompatible?' in *Taveners.*

[48] A Acquisti, 'Awareness, Understanding, and Individual Decision-Making', *OECD Conference.* Heinz College/CyLab, Carnegie Mellon University, October 26, 2010, <http://www.oecd.org/dataoecd/33/40/46943626.pdf>.

2 Defining Privacy: the ever-changing concept

Privacy is a multifaceted concept[49] that, as have been demonstrated above, is currently seriously challenged by the overall technological developments and mostly by the growth of the SNSs.[50]

The concept of privacy has always been subjected to changes.[51] Patterns of privacy may differ significantly from society to society, depending on social, cultural, political factors, as well as on the historical situation.[52] Moreover, privacy is often balanced against other values.[53]

All these factors make the concept of privacy difficult to define. The list of its possible definitions seems to be endless.[54] Nevertheless, the lack of a single definition should not imply that the issue lacks importance.[55] Quite on the opposite.

Some of the viewpoints on privacy given below demonstrate different approaches, which are taken in the literature in defining a rich and quite controversial phenomenon, which is privacy. As a legislative approach to the notion is analysed in the next chapter, the current one attempts to conceptualize privacy from a more theoretical, academic angle.

Outside of the strict context, privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs[56] or

---

[49] M Friedewald, 'A New Concept for Privacy in the Light of Emerging Sciences and Technologies', *From the SelectedWorks of Michael Friedewald*, April 2010, p. 71, <http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=michael_friedewald>.

[50] C Vegheş, C Pantea, D Bălan & B Lalu, 'European Union Consumers' Views on the Protection of their Personal Data: an Exploratory Assessment', *Annales Universitatis Apulensis Series Oeconomica*, 11(2), 2009, p. 989, <http://oeconomica.uab.ro/upload/lucrari/1120092/44.pdf>.

[51] Friedewald, p. 71.

[52] Zwick & Dholakia, p. 9.

[53] Friedewald, p. 71.

[54] M Foutouchos, 'The European Workplace: The Right to Privacy and Data Protection', *Accounting Business & the Public Interest*, vol. 4, No. 1, 2005, p. 38, <http://visar.csustan.edu/aaba/Foutouchos.pdf>.

[55] C Laurant, *Privacy & Human Rights 2003: An International Survey of Privacy Laws and Developments*, Electronic Privacy Information Center, Washington, DC, USA, Privacy International, London, UK, 2003, <https://www.privacyinternational.org/survey/phr2003/index.htm>.

[56] ibid.

as a restriction of information diffusion.[57]

One of the first definitions, and apparently one of the most broadly accepted, is that privacy is "the right to be let alone".[58] It has been made in the 1890s by a future United States Supreme Court Justice Louis Brandeis.

Schoeman defined privacy as a claim, entitlement or right of an individual to determine what information about himself may be communicated to others; the measure of control an individual has over information about himself.[59]

According to Robert Ellis Smith, an editor of the Privacy Journal, privacy is a "desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves."[60]

Edward Bloustein looked at privacy as at an interest of the human personality, which protects the inviolate personality, the individual's independence, dignity and integrity.[61]

According to Ruth Gavison, there are three elements in privacy: secrecy, anonymity and solitude. It is a state which can be lost, whether through the choice of the person in that state or through the action of another person.[62]

Furthermore, Alan Westin[63] has defined privacy as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[64]

Similarly, privacy has been conceived as "the individual's ability to control the circulation of information relating to him",[65] or, alternatively, the right

---

[57] Zwick & Dholakia, p. 9.

[58] Laurant.

[59] Vegheş, Pantea, Bălan & Lalu, p. 988.

[60] R E Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, Sheridan Books, 2000, p. 6, cited in Laurant.

[61] 'Privacy as an Aspect of Human Dignity', *New York University Law Review*, vol. 39, 1964, cited in Laurant.

[62] R Gavison, 'Privacy and the Limits of Law', *Yale Law Journal*, vol. 89, No 3, January 1980, cited in Laurant.

[63] Professor of Public Law at Columbia University, a former publisher of *Privacy & American Business.*

[64] A Westin, *Privacy and Freedom*, London, Bodley Head, 1967, p. 7, cited in Foutouchos, p. 37.

[65] A R Miller, *Assault on Privacy: Computers, Data Banks and Dossiers*, Michigan, MichiganUP, 1971, p. 40, cited in Foutouchos, p. 37.

to know about and to control what information is being held on an individual.[66]

Additionally, privacy is claimed to be a right complementary to all other sorts of rights, in the sense that if not enjoyed freely there can be chilling effects to the exercise of other kinds of rights.[67]

As Daniel J. Solove argues, despite of the seeming endless of different privacy definitions, the debate may actually help in revealing several principal directions of conceptualizing privacy. Thus, Solove outlines six of them:
(1) a well-known and already cited before Louis Brandeis's approach to privacy as to the right to be let alone;
(2) limited accessibility – the ability to shield oneself from unwanted access by others;
(3) secrecy – the concealment of certain matters from others;
(4) information control – the ability to exercise control over information about oneself;
(5) personhood – the protection of one's personality, individuality, and dignity; and
(6) intimacy – control over, or limited access to, one's intimate relationships or aspects of life.
Some of the formulations concentrate on means to achieve privacy; others focus on the ends or goals of privacy. Further, there is a certain overlap between conceptions, and the conceptions discussed under different headings are by no means independent from each other.[68]

Nevertheless, what can be concluded from the Solove's approach in looking at privacy from different angles is the following: when we state that we are protecting "privacy", we are claiming to guard against disruptions to certain practices, while the practices in turn may be disrupted in certain ways.[69]

Similar with this "disruptions to certain practices" approach is an attempt to define privacy through the three "zones" in need of protection.[70] The first one deals with territorial or spatial aspects (e.g. privacy within somebody's home). The second zone - with person as such, linking privacy exclusively to intimate or sensitive aspects of ones' life. Finally, the last 'zone' of

---

[66] J Michael, *Privacy*, in D Harris & S Joseph, *The International Covenant on Civil and Political Rights and United Kingdom Law*, London, Clarendon Press, 1995, pp. 267-272, cited in Foutouchos, p. 37.

[67] J Michael, *Privacy and Human Rights: An International and Comparative Study, With Special References to Developments in Information Technology*, Dartmouth: UNESCO Pub., Aldershot: Paris, 1994, p. 4, cited in Foutouchos, p. 38.

[68] D J Solove, M Rotenberg & P M Schwartz, *Privacy, information, and technology*, Aspen Publishers, 2006, p. 44.

[69] ibid.

[70] Foutouchos, p. 37.

privacy is understood in the terms of information control.[71]

While talking about privacy in the last aspect it is more appropriate to operate with the notion of "information privacy". Not surprisingly, in the digital age the third zone of privacy and its "informational dimension" has become the primary focus of public attention and legislative development.[72]

The following definition of information privacy may be provided here: it is an interest that individuals have in controlling, or at least significantly influencing, the handling of personal data about themselves. The term "data privacy" is sometimes used in the same way. The notion emerged during the mid-1960s, and the growth of its importance is often perceived to be directly linked to the development of computer technologies.[73]

An understanding of privacy through its third, "information", zone constitutes a particular importance for the current research, as it deals directly with the law and policy on information privacy and data protection.[74]

The definition of privacy in this context would remain insufficient without a better understanding of what exactly counts as private information.[75] However trivial it may sound, yet a definition given by Stanley Benn in 1971 clearer than anything else explains the core idea behind private information. He defined the last by referring to a simple example - a couple kissing in the bushes to hide from the public, thus acting privately, or in private. Although the couple's act may have meant to be a private affair, the two could later decide to share this experience with someone else, at which point the private matter becomes public. Benn believes that "it is not that the information is kept out of sight or from the knowledge of others that makes it private." Rather, what matters is that it would be inappropriate for others to try to find out about, much less to report on this information, without the couple's consent.[76]

Such a definition, apart from precisely capturing the essence of privacy itself, seems to be a good response to the claims of those, who, in line with

---

[71] L A Bygrave, 'Privacy and Data Protection in an International Perspective', *Stockholm Institute for Scandinavian Law*, 2010, p. 170, <http://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Privacy%20and%20Data%20Protection%20in%20International%20Perspective.pdf>.

[72] R Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms', in *Roger Clarke's Web-Site*, 15 August 1997, viewed on 7 May 2011, <http://www.rogerclarke.com/DV/Intro.html>.

[73] ibid.

[74] Bygrave, p. 170.

[75] Zwick & Dholakia, p. 9.

[76] S I Benn, *Privacy, Freedom, and Respect for Persons*, in R J Pennock & J W Chapman (Eds.), Privacy (pp. 1-26). New York: Atherton Press, 1971, p. 2, cited in Zwick & Dholakia, p. 9.

Google's CEO Eric Schmidt, try to operate with "nothing to hide, nothing to fear" arguments while touching upon the privacy issues on the social networking platforms.[77] Clearly, wanting private space is not about hiding something wrong or shameful. It's about maintaining individuality and liberty. Some things aren't wrong. They are just private.[78]

Stopping here on the theoretical discourse about the nature of privacy (which otherwise risks to be endless) let's turn to the relevant European law on the matter of information privacy protection. The following chapter, thus, focuses on the origins and development of the right to privacy and personal data protection in Europe and their implications in the sphere of social networking.

[77] See the previous chapter.

[78] One online commentator had a nice retort for the Google CEO: "I planted a microphone in Eric Schmidt's bedroom (it's broadcasting live on my blog). I'm sure he won't mind, as he surely isn't doing anything he wouldn't want anyone to know about." Stoddart, 'Why Privacy Still Matters'.

3 Historical development of Privacy and Data protection legislation: the basis and evolution in Europe

The current chapter outlines the set of the relevant legal norms on the European information privacy area. The European legal order of privacy and data protection encompasses the EU data protection regime and relevant law of the Council of Europe. The EU regime comprises four directives, one regulation, as well as Articles 7 and 8 of the EU Charter,[79] while the main legal instruments of the Council of Europe in the context under discussion include the ECHR (Article 8) and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 (Convention 108).

The modern European history of the right to privacy starts after the Second World War. Initially, privacy protection in Europe was driven by the desire to prevent States from using personal data for the purposes of executing malicious policies, as had happened in Nazi Germany and other totalitarian States.[80] The world tired from two global wars was in need for some fundamental rights so as to be able to live without fear of arbitrary interference from the States.[81]

In 1950 a fundamental right to "respect for private life" was included in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).[82]

The relative right was to be construed in two paragraphs: one would contain

---

[79] N Purtova, 'Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights'. *Netherlands Quarterly of Human Rights*, vol. 28, No 2, 2010, pp. 179-198, p. 5, <http://arno.uvt.nl/show.cgi?fid=106377>.

[80] L Bergkamp, 'EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy', *Computer Law & Security Report*, vol. 18, No. 1, 31 January 2002, pp. 31-47, <http://www.hunton.com/files/tbl_s47Details/FileUpload265/499/Privacy_fallacy.pdf>.

[81] Foutouchos, p. 40.

[82] Article 8 ECHR reads as follow:

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

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

the right itself and one the derogations.[83]

As to the potential effects of automatic data processing upon the right to privacy,[84] the Council's concern with this regard began to grow only after the ECHR had been adopted. It had been triggered by the advances in information technology during the early 1960s and the early 1970s.[85]

By that time the European States started to introduce, on a national basis, legislation concerning protection of personal data and thus of private life. Such an independent and sporadic legislation turned to be problematic,[86] as the disparities in national privacy legislation created obstacles to the free flow of information between countries. Harmonization of national privacy legislation, along with the protection of individual privacy interests in personal data, became a major purpose of privacy activities held by international organizations.[87]

On the European level the three main institutions attempted to solve this problem:
1. the Council of Europe (COE), that had the experience in protecting privacy with the ECHR;
2. the Organisation for Economic Cooperation and Development (OECD); and
3. the European Economic Community (EEC) (later – the European Community – EC and after – the European Union - EU), which mainly had economic orientation.[88]

The cooperation of the OECD and of the COE resulted with the adoption of the Convention 108 in 1981.[89] It drew inspiration directly from Article 8 of the ECHR.[90] The Council of Europe Convention 108 established the data subject's right to privacy, enumerating a series of basic principles for the data processing.[91] Besides, it stated that "it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow

[83] Foutouchos, p. 40.

[84] R Gellman, 'Fair information practices: A Basic History', Version 1.82, April 19, 2011, pp. 4-7, <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>.

[85] Foutouchos, p. 42.

[86] ibid.

[87] Gellman, pp. 6-7.

[88] Foutouchos, p. 42.

[89] ibid., pp. 42-43.

[90] Jagland, p. 4.

[91] J Slemmons Stratford & J Stratford, 'Data Protection and Privacy in the United States and Europe', *IASSIST Conference*, Yale University, New Haven, Connecticut, May 21,1998, p. 19, <http://www.iassistdata.org/downloads/iqvol223stratford.pdf>.

across frontiers of personal data undergoing automatic processing."[92]

Around the same time as the Convention 108 was introduced, the OECD proposed similar privacy guidelines, seeking to ensure the free flow of economically necessary personal information by proposing standards that would harmonize different national data protection and privacy legislation schemes.[93]

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data became applicable in 1980.[94] Although being of a "soft law" nature, the Guidelines exercised a considerable influence on the development of data protection law.[95] The Guidelines, compared to the Convention 108, placed a major emphasis on the economic development rather than on human rights and fundamental freedoms (as the Convention 108 did).[96]

By the time the Convention 108 and the OECD Guidelines had been introduced it was still the childhood of the modern data technology. This was a time without Internet, without Facebook, with no Twitter and no laptops. However, it was a time when huge computers used by public administrations and big enterprises became a way of doing business.[97]

Although the Member States did sign the Convention 108, only six had ratified it by 1990. So, in the early 1990s the EU got worried about the discrepancies among national data protection laws that disrupted the function of the common market.[98]

To face these problems 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 (the Data Protection Directive) was enacted by the EU in October 1995. It reaffirmed the principles established by the Council of Europe Convention 108 and putted down a broad regime of data protection.[99]

The Data Protection Directive set a milestone in the history of the protection

---

[92] Gellman, p. 5.

[93] M T D Gray, J Hester & J E Cole, *Uniform Standards to Protect the Privacy of Personal Information: A Study of the International Trend to Protect Privacy in Personal Information*, Office of Information Practices, January 2000, p. 2, <http://www.state.hi.us/oip/reports/privrptappb.pdf>.

[94] Gellman, p. 5.

[95] Bygrave, p. 183.

[96] Gray, Hester & Cole, p. 2.

[97] Jagland, p. 3.

[98] Foutouchos, p. 44.

[99] Bergkamp.

of personal data in the European Union.[100] Its major components acknowledged the individual's right to privacy, setting important standards for the treatment of personal data collected from individuals. The Directive called for the member states to bring their national privacy laws into compliance within three years.[101] In addition, it restricted the export of personal information to third countries that did not ensure an "adequate level of protection". This encouraged some other countries to conform their laws to the principles that formed the basis of the directive.[102]

After its adoption the Data Protection Directive had been supplemented by several EU sectoral Directives, dealing with specific issues of data protection.[103]

The first of these was Directive 97/66/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.[104] It has been followed by ePrivacy Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.[105] The Data Retention Directive 2006/24/EC6[106] was then passed in 2006, modifying the impact of the Directive 2002/58/EC by requiring the EU Member States to ensure that providers of public communications networks retain traffic and location data for a certain period – namely, for a minimum of 6 months and maximum of 2 years.[107]

Additionally, the EU has adopted a Data Protection Regulation 45/2001/EC4,[108] which complemented the Data Protection Directive and laid down specific data protection rules with regard to the Community institutions and bodies.[109]

---

[100] European Commission, *A comprehensive approach on personal data protection in the European Union*, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee of the Regions, Brussels, 4 November, 2010, COM(2010) 609 final, p. 2, <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf>.

[101] J Slemmons Stratford & J Stratford, p. 19.

[102] Gellman, p. 7.

[103] Bygrave, p. 185.

[104] Adopted 15th Dec. 1997 (O.J. L 24, 30th Jan. 1998, p. 1 *et seq.*).

[105] Adopted 12th July 2002 (O.J. L 201, 31st July 2002, p. 37 et seq.).

[106] Directive 2006/24/EC of 15th 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 (O.J. L 105, 13th April 2006, p. 54–63).

[107] Bygrave, p. 185.

[108] Regulation (EC) 45/2001 of 18th Dec. 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 (O.J. L 8th Dec. 2001, p. 1 *et seq.*).

[109] Docksey, p. 2.

What is especially important, at the constitutional level, the EU Charter of Fundamental Rights of 2000[110] both updated the right to privacy and placed the right to data protection in the separate article.[111]

As the Lisbon Treaty was signed by the EU Member States in 2007 and entered into force on 1 December 2009, the Charter became legally binding.[112] The main result of its new "hard-law" nature is a recognition of the protection of personal data as a self-standing fundamental right (in Article 8 of the Charter)[113] with a full legal validity as a part of primary EU law. It means that data protection will play a more important role when balanced with other values and interests (e.g. market interests), and when priorities are to be defined by, among others, the ECtHR.[114]

As to the nearest future, it has to be pointed out that the Commission has launched a review of the current legal data protection framework.[115] A number of studies were initiated as well.

***

Summing up, as has been demonstrated through this brief historical legislative review, privacy law and data protection law have emerged from a common point of view; they both tried to protect the right to privacy of the individual, either against the state (ECHR) or against the private sector (EU and COE legislation). However, there is a crucial difference: data protection legislation emerged not only for the protection of the individual, but also for the free flow of data among the European countries, that is so much needed for the undisrupted function of the common market. In other words, data protection law did have the essence of protection of a fundamental right (privacy), but also it was meant to be company friendly.[116]

Nevertheless, the last consideration doesn't exclude this paper's idea that the right to privacy and data protection are in a sense two sides of the same

---

[110] EU Charter of Fundamental Rights of 7 December 2000.

[111] Docksey, p. 2.

[112] F Le Bail, 'Discours d'ouverture', *Speech on the Data Protection Day*, Brussels, 28 January 2011, p. 3, <http://www.data-protection-day.net/files/Introduction_0_3_Francoise_Le_Bail_speech_FINAL_OK_FOR_WEBSITE.pdf>.

[113] ibid.

[114] European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*, Publications Office of the European Union, Luxembourg, 2010, p. 18, <http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf>.

[115] Le Bail, pp. 1-2.

[116] Foutouchos, p. 44.

coin:[117] the one was meant (at the time when the legislation appeared) to be applicable to the public sector, whilst the other – to the private one.[118]

The need to prove this idea calls for a comparative analysis of the right to privacy and data protection, as well as of the place of the last one in the case law of the ECtHR.

[117] ibid., p. 43.

[118] As to be demonstrated further, the dynamic interpretation of the ECHR case law currently calls for an applicability of the Strasbourg Convention to the private sector as well (though only indirectly).

4 On the relationship between "Privacy" and "Personal Data Protection"; Property v. Human right

There are various ways to consider data protection[119] and there are even more when it comes to defining its correlation with the right to privacy.

Nevertheless, it is possible to outline the two main theoretical approaches to the issue of the relationship between privacy and data protection: theoretical attitudes, as well as the legal policies and practices across the globe are either in favor of treating data protection as consumed by or largely intersecting with privacy, or, alternatively, treat the two categories as absolutely distinct.[120]

These standpoints rest on different ways of conceptualizing information privacy[121] and the two different privacy philosophies, which have evolved on either side of the Atlantic.[122]

In the USA privacy in personal data is considered as a property right, as opposed to the European model, granting personal data a level of human rights protection.[123]

First of all, a few words should be said in order to explain why this comparison is actually important for the purposes of the current paper.

The comparative analysis of data protection and privacy predetermines, among others, the character of rights over personal data (including personal information the users of the social networking platforms provide in exchange for the services) in relation to the principle of freedom of contract.[124]

The current chapter's analysis goes to prove that data protection (at least in Europe) is a part of a fundamental right to privacy, and that, therefore, it

---

[119] C de Terwangne, 'Is a Global Data Protection Regulatory Model Possible?', in *Reinventing Data Protection?*, S Gutwirth, Y Poullet, P De Hert, C de Terwangne & S Nouwt (eds), Springer, 2009, p. 180.

[120] Purtova, 'Private law solutions in European data protection', p. 3.

[121] ibid.

[122] Zwick & Dholakia, p. 11.

[123] ibid., pp. 16-17.

[124] Cuijpers, p. 306.

should be protected accordingly, meaning placing a ban on its waiver on the basis of freedom of contract.

4.1 American model: Personal Data as a property right (outside of the scope of Article 8 ECHR protection)

There is a profound evidence (based on the legislation, as well as on the academic works and political debates) that in the USA personal data (or, to put it differently – information privacy or personal information) are seen as a property right rather than a human right, a commodity that is tradable. Hence, an American legal system treats personal data as a private property.[125]

The idea of a proprietary nature of personal information is not a new one. It has a long history in legal as well as sociological thought,[126] though many of the arguments that have been forwarded in its favor derive from American sources.[127] For this reason the model under which data protection is viewed as a property right and is regarded separately from the right to privacy has received in the literature the name of an "American model".

The approach to data privacy under this model is shared, among others, by Alan Westin,[128] who states that "personal information, thought of as the right of decision over one's private personality, should be defined as a property right".[129] Edward Shils goes even further in saying that "the social space around an individual, the recollection of his past, the conversation, his body and its image, all belong to him".[130] The intention of such definition was to provide the carrier of personal information with the right to sue when there was information abuse.[131]

A suggestion is expressed by the proponents of vesting a property right in

---

[125] A Busch, 'From Safe Harbour to the Rough Sea? Privacy Disputes across the Atlantic', *SCRIPT-ed*, vol. 3, issue 4, June 2006, p. 318 , <http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/busch.asp>.

[126] Zwick & Dholakia, p. 16.

[127] Prins, p. 2.

[128] Westin's research at Columbia University in the 1960s is widely seen as the first significant work on the problem of consumer data privacy and data protection. Westin's academic works on privacy has influenced significantly the USA privacy legislation. He has also specialized in studying the impact of information technologies on national and local governmental operations.

[129] A R Miller, *The Assault on Privacy*, Ann Arbor: The University of Michigan, 1971, p. 211, cited in Zwick & Dholakia, p. 16.

[130] Miller, p. 212, cited in Zwick & Dholakia, p. 16.

[131] ibid.

personal data that individuals do 'own' their privacy in a certain sense, since personal data rights are tightly connected with ownership and control and, as such, these rights are alienable: they can be waived or 'sold'.[132]

Such an approach allows individuals to make individualized deals for trading the right to use their personal data against preferential services, money, or other benefits[133] (in our case – against benefits of using social networking platforms on-line). Personal information defined as a commodity, therefore, means that the individual consumer holds the right for commercial exchange of his or her own information privacy in the marketplace. Companies interested in personal data collection can then offer a price to the consumer, thus copying, albeit in inverted roles, a regular commercial transaction.[134]

As to the reasons, explaining an appearance and consequent development of the examined information privacy model in the USA, they may be seen in a long liberal tradition, combined with no less long tradition of distrust against the government on the American ground.[135] The State there is reluctant to interfere with the space where the private business operates, and a lot is left to the self-regulation. This market-oriented approach hardly accepts imposing "burdens" on economic activities in the name of the protection of personal data.[136] The private sector and free market are seen as the most effective mechanisms for protecting information privacy, with the focus being more on the consumer than on the citizen. Accordingly, protection is often more reactive than proactive[137] here.[138]

Thus, following the USA model, personal data becomes an exchangeable property and the possessor of property presumably makes rational choices as to how, when, with whom, and for what price he or she wants to trade it.[139] Data protection turns into a consumer concern,[140] with the last having a free choice in exchanging personal information in the market, thereby deciding upon the degree to which he or she wishes to protect his or her privacy.[141] The protection here is to be balanced with private interests.[142] With the

---

[132] Prins, p. 10.

[133] ibid, p. 9.

[134] Zwick & Dholakia, p. 16.

[135] Busch, p. 309.

[136] Terwangne, p. 188.

[137] Busch, p. 318.

[138] One can call to mind here the quotation given before about Facebook not asking for permission, but for forgiveness.

[139] Zwick & Dholakia, p. 18.

[140] Terwangne, p. 181.

[141] Zwick & Dholakia, p. 18.

[142] Terwangne, p. 181.

definition of privacy as of a commodity, personal data can be treated according to the economic laws of the marketplace and without direct normative interference from other authorities.[143]

Far from this perspective, data protection approach implemented on the European ground (and reflected in the EU and Council of Europe legislation), considers information privacy as something quite different.[144]

4.2 European model: Personal Data as a Human Right (and part of the Right to Privacy as enshrined in Article 8 ECHR)

In the European legal order there is a conclusive evidence in favor of treating data protection interests as an integral part of a more general right to privacy with a consequence of data protection interests enjoying the full scope of a fundamental human right status.[145]

The European model sees the right to data protection as an inalienable civil right,[146] as a precondition for the individual's autonomy that cannot be commodified and traded away on the marketplace.[147]

Historical experiences with the dictatorships such as the Nazis (who used census data for the holocaust) and repressive regimes in the Eastern Europe have sensitized Europeans to the importance of data protection.[148]

Defined as a civil right, information privacy escapes the consequences of commercialization and cannot be owned by anyone in an economic sense, only in a political.[149] Thus understood, information privacy imposes the burden of its protection not on the individual, but on the society.[150] It must be protected by the State or any other legislative system in charge of protecting the rights of its citizens against violation.[151] Therefore, the European model of reinforcement of data privacy is regulatory, as opposed to the USA self-regulatory standards.

---

[143] Zwick & Dholakia, p. 20.

[144] ibid, p. 17.

[145] Purtova, 'Private law solutions in European data protection', p. 3.

[146] Zwick & Dholakia, p. 17.

[147] Busch, p. 318.

[148] ibid.

[149] Zwick & Dholakia, p. 14.

[150] Busch, p. 318.

[151] ibid.

Under the European model marketers, as well as consumers have only little freedom to interact on the matter of privacy. Only legislative regulations can safeguard it. Privacy in personal data is, therefore, irreducible to the individual property principle, and personal information cannot be commodified.[152]

Seeing data protection as a fundamental right clearly reflects the Council of Europe's approach and the EU's approach in general: the Council of Europe Convention 108 and Articles 7 and 8 of the EU Charter are evident human rights instruments.[153] In addition, the EU policies behind the Data Protection Directive 1995 are predetermined by the established view on privacy as a human right. A general argument of the Directive is that the reliance on the recognition of a property right of personal information would have the undesirable consequence of placing responsibility on each individual to protect his or her own interest. Without an external authority imposing and enforcing regulations on business, the individual user's interest in protection and the businesses' interest in data collection are in direct conflict, with the business organizations having a superior position in the unequal bargaining process.[154]

Information privacy (or the right to the protection of personal data) under the European model is conceived, therefore, as a fundamental component of a more broad right to privacy. As the last is largely safeguarded by means of the Article 8 ECHR, data protection should also benefit from a shielding power of the basic human rights instrument, which the Convention is. Personal consumer information, as a result, cannot be exchanged in the marketplace, but must be protected from exploitation. For business the consequence is in clear delimitation of data collection possibilities with a small room for interpretation.[155]

Reflecting on the named significant differences between the European and the American models of information privacy, Yale law professor James Whitman has accurately named them as "Dignity versus Liberty" respectively. Describing the European privacy culture operating by the notion of dignity, he pointed out that in Europe "one's privacy, like other aspects of one's honor, was not a market commodity that could simply be definitively sold."[156] According to Whitman, "any sale by a person who had momentarily 'forgotten his dignity' had to remain effectively voidable."[157]

---

[152] Zwick & Dholakia, p. 20.

[153] Terwangne, pp. 180-181.

[154] Zwick & Dholakia, p. 17.

[155] ibid., p. 20.

[156] B Sullivan, ''La difference' is stark in EU, U.S. privacy laws', in Privacy Lost on msnbc.com, 19 October 2006, viewed on 8 May 2011, <http://www.msnbc.msn.com/id/15221111/ns/technology_and_science-privacy_lost/>.

[157] Cited in Sullivan.

Similarly to Whitman, Deborah Hurley goes to state that "in Europe privacy and personal data protection is regarded as an inalienable right because it is so important to [their] dignity and sense of autonomy."[158] Under such a position personal information is not to be owned as much as protected, and the authority regulating privacy is, of course, the State.[159]

It turns to be clear now (specially in the light of a recent expansion to the European marketplace of the online social networking business, created under the USA model) that the European standpoints on the matter of online data privacy are diametrically opposed to that of the US administration and business groups.[160]

4.3 Arguments against treating Personal Data as a human right under the European model

The first piece of argumentation was aimed to demonstrate the discrepancies in the way personal data are treated in Europe and the USA.

Nevertheless, it can't be avoided mentioning that there are also some arguments raised in the literature in favor of proving that, under the European legislative system, there is as well a flour to treat personal data in accordance with an American model.

The theorists standing behind such line of argumentation contend that data protection interests as such (either in Europe, USA or anywhere else) are not to be considered as part of a fundamental human right to privacy: privacy is portrayed by those authors as a purely defensive mechanism against intervention into some secluded personal sphere. Privacy protection mechanisms, according to those claims, are unable to take care of personal data protection, which requires more 'offensive' approach – not prohibiting, but channeling processing of personal information. For that reason, they argue, data protection considerations are not powerful enough to serve as a ground for legitimate restrictions of freedom of contract. The latter, when balanced against data protection interests, has precedence, and data protection rules can be contracted around freely.[161] In other words, in the contract one is free not to abide by the data protection requirements.[162]

---

[158] D Hurley, 'Privacy in Play', *Think Leadership Magazine*, 1998, cited in Zwick & Dholakia, p. 17.

[159] Zwick & Dholakia, p. 17.

[160] ibid.

[161] Purtova, 'Private law solutions in European data protection', p. 2.

[162] Cuijpers, pp. 312-315.

It is claimed, accordingly, by those denying a human rights nature of the right to data protection that information privacy in the framework of the European legislation should be viewed outside of the scope of Article 8 ECHR.

The two main arguments are provided in order to support this claim.

The first deals with the substance of protection by Article 8 ECHR, namely, it is argued that the named article protects only privacy as secrecy, i.e. concerns only concealed personal information, and prevents collection, but not other information practices.[163]

The second argument appeals to the mode of protection and goes to state that Article 8 ECHR does not apply to private parties and does not contain positive obligations.[164]

In this context, the point of view developed by Peter Blok and supported by Colette Cuijpers is of a special interest.

Peter Blok challenges the constitutional character of the right to data protection as opposed to the right to privacy.[165] According to Blok, privacy can be defined as follows: "The individual right to privacy both safeguards an undisturbed private life and offers the individual control over intrusions into his private sphere. Given this definition, the boundaries of the private sphere are central to the meaning of privacy. The right to privacy guarantees individual freedom within the home, within the intimate sphere of family life, and within confidential communication channels. In combination with physical integrity, these 'privacies' form the core of the legally protected private sphere."[166]

As the individual's protection with regard to the processing of personal information is in no way restricted to data concerning his or her private sphere, Blok concludes that the choice to link data protection to the right to privacy is made unjustly.[167]

Supporting Blok's argument, Colette Cuijpers says that data protection is not a fundamental right. Therefore, freedom of contract has precedence over the rules of the EU Data Protection Directive, and the right to data protection may be waived or contracted around.[168]

---

[163] Purtova, 'Private law solutions in European data protection', p. 7.

[164] ibid.

[165] Cuijpers, p. 312.

[166] P Blok, Het recht op privacy (The right to privacy), The Hague: Boom Juridische Uitgevers 2002, cited in Cuijpers, p. 312.

[167] Blok, cited in Cuijpers, p. 312.

[168] Cuijpers, pp. 304-318.

As to the viability of such argumentation, it is hard not to agree with Nadezhda Purtova's comment: "The general feeling one gets after reading Blok's and Cuijpers' argumentation is that the Art. 8 ECHR jurisprudence should not have gone so far to extend the right to privacy beyond the text of the Convention and thus diminishing the importance of the right that was originally meant to be protected. That is in essence a normative statement pointing at the way the jurisprudence *should* have gone."[169]

Nevertheless, it's not the task of the current analysis to go into consideration of the directions in which the jurisprudence of the ECtHR could have gone. The fact is that it has chosen to develop in the direction of recognition of a human rights nature behind personal data, and the reality is that this model is already actualized by the European Union.[170] The scope of Article 8 ECHR right to privacy has been broadened in the case-law of the Strasbourg Court over time to make it possible to overturn both the arguments with regard to the substance and the mode of the Convention privacy protection. Article 8 ECHR by now has been interpreted extensively to let data protection interests be embraced by it. Moreover, the current Court's jurisprudence recognizes the existence of positive obligations of the States in the context of, among others, the right to privacy, therefore making Article 8 ECHR applicable (though indirectly) to private parties.

Whether it was a right or wrong direction for the Court to choose is, again, not the issue of the current research. Furthermore, the author doubts that the answer to this question can be found at all, as it is a matter of policy and the whole cultural, historical, political and legal heritage of the European community. Acknowledging that the theoretical debate on the meaning of privacy and its relation to data protection is unlikely to end soon, it seems to be reasonable to focus on the actual legal rules in practice.[171]

With this rational in mind the current paper will refer to Article 8 ECHR for guidance, which can be helpful in resolving the confusion and proving, as a result, that the human rights issues cannot be avoided in the data protection debate.[172]

The following subchapter aims at demonstrating, opposing to the arguments of those distinguishing privacy and data protection, that, when it comes to actual application of law, the ECtHR does not limit the scope of Article 8 ECHR to private sphere only, and the provision on privacy protection has been applied as giving individuals data protection rights and imposing on the States positive obligations. Accordingly, it is to be demonstrated that in legal practice (as opposed to academic debate) there is no ground to treat

---

[169] Purtova, 'Private law solutions in European data protection', p. 4.

[170] Zwick & Dholakia, p. 17.

[171] Purtova, 'Private law solutions in European data protection', p. 3.

[172] ibid., p. 2.

data protection distinctly from privacy rights.[173]

4.4 Actual legal practice: Human Rights nature of the right to Data Protection in Europe; Ban on the waiver of the right

The general tendency for the evaluation of the fundamental right to privacy can be seen in the related case law of the Strasbourg Court and its evolution over time.[174]

It is true that the early years of the application of the ECHR (in 1950s, when the Convention was adopted, or in 1968 when its applicability to data protection was evaluated), respect for private and family life as enshrined in Article 8 ECHR might have contained only a negative right meant to protect an individual's private sphere from the State's intervention.[175] Consequently, the invasion of privacy at that time was largely justified under Article 8(2) ECHR, while the scope of the right to privacy under this article was interpreted in a narrow sense.[176] It also may be true that at that time and at that stage of the society's development (together with the development of information technologies) the question of interpretation of data protection as being part of Article 8 ECHR wasn't and simply couldn't be the most important one on the European agenda. In fact, who could imagine at that time the way in which the Internet will literarily change the world around?

But it did, and, as the years went by, the right to privacy as enshrined in Article 8 ECHR started to be considered a more and more fundamental, and its scope broadened.[177] At present there is profound evidence on the European level confirming inclusion of data protection right into the scope of Article 8 ECHR.

This extension of the original scope of Article 8 ECHR has been made possible because the Convention is deemed as a "living instrument" which ought to be interpreted only in an extensive way.[178] "The Contracting Parties signed in full knowledge that ideas and morals [behind the

---

[173] ibid., p. 5.

[174] Foutouchos, p. 41.

[175] Purtova, 'Private law solutions in European data protection', p. 7.

[176] Foutouchos, p. 41.

[177] ibid.

[178] See on these points, notably *Tyrer* v. *UK* and *Selmouni* v. *France* cases, cited in Y Poullet, in *Council of Europe BLOGGED Submission to the Internet Governance Forum*, Athens, Greece, 30 October to 2 November 2006, p. 5, <http://www.coe.int>.

Convention's interpretation] would change and that the meaning of the Convention would keep pace."[179]

This leads progressively to consider that the protection of all data, that might be viewed as "the informational image of the individuals", has to be ensured, and not only the sensitive ones.[180] In other words, with the development of its case law over time the protection of Article 8 ECHR went beyond concealed personal information.[181]

Since the mid-1990s the ECHR case law has been following the idea of privacy as encompassing more then just secrecy[182], but as well personality rights.[183]

An inclusion of data protection in the EU Charter confirms the above-given considerations on the human rights foundations[184] of the information privacy.[185]

To be sure, the EU Charter does distinguish a right for respect for private and family life (Article 7) and a right to personal data protection (Article 8). The inclusion of the last one under the separate heading of Article 8 of the Charter was inspired, inter alia, by the Directive 95/46/EC as well as by Article 8 of the ECHR and by the Council of Europe Convention 108.[186]

To prevent a possible speculation (about different nature of the two rights) on the ground of the Charter's inclusion of the right to privacy and right to personal data protection into two separate articles, it should be noted that the same it does with regard to equality between men and women (Article 23) and a right to non-discrimination (Article 21), whereas the ECHR deals with those two in a single provision - Article 14 ("Prohibition of discrimination"). The analogy allows for a simple conclusion that it is merely a chosen technique of the Charter to deal with special instances of more general rights separately in order to ensure their more adequate

---

[179] R Beddard, *Human Rights and Europe*, Cambridge University Press, 1994, cited in Purtova, 'Private law solutions in European data protection', p. 7.

[180] Y Poullet, in *Council of Europe BLOGGED Submission to the Internet Governance Forum*, p. 19.

[181] Purtova, 'Private law solutions in European data protection', p. 7.

[182] ibid.

[183] See, for instance, the case of *Reklos and Davouris* v. *Greece*. ECHR 15 April 2009, *Reklos and Davourlis* v. *Greece*, Application no. 1234/05.

[184] Bergkamp.

[185] Article 8 of the EU Charter provides that "everyone has the right to the protection of personal data."

[186] *Explanations relating to the Charter of Fundamental Rights*, prepared under the authority of the Praesidium of the Convention which drafted the Charter of Fundamental Rights of the European Union, 2007/C 303/02, <http://eur-lex.europa.eu/en/treaties/dat/32007X1214/htm/C2007303EN.01001701.htm>.

protection. In any case, separation of a right for respect for private and family life and a right to data protection in the Charter does not exclude interpretation of data protection as a part of a general right to privacy.[187]

Therefore, this paper argues that the European approach rests on the assumption that, legally speaking, data protection is an element of the fundamental right to privacy as secured by Article 8 ECHR, and therefore enjoys a full protection of a fundamental rights status.[188]

As a part of such protection, it is an established position of jurisprudence[189] and the literature that the ECHR does not protect a right to obtain remuneration for the waiver or sacrifice of a fundamental right, as an individual cannot claim a violation when the State prevents him or her, e.g. via regulation, from waiving a fundamental right.[190]

Transactions in which individuals waive their entitlement in personal data in return for remuneration or services (as is the case with social networking) shouldn't be enforceable on the level of the ECHR.[191]

An important remark has to be made here. This paper *does not* argue that contractual arrangements, concerning personal data, as has been fairly noted by Nadezhda Purtova, are altogether impossible under the Convention. However, the consequence of classification of data protection as a fundamental right protected under Article 8 ECHR limits the scope of the allowed contractual arrangements and possible property rights.[192]

To understand this point better one has to think of the content of the right discussed here. Data protection does not mean non-disclosure and total secrecy of personal information. It rather channels the operations with personal information and controls them by, *inter alia*, imposing on the States positive obligations.[193] Only one example of such a tool of channeling information practices in the Data Protection Directive is a

---

[187] Purtova, 'Private law solutions in European data protection', p. 6.

[188] N Purtova, 'Property in Personal Data: a European Perspective on the Instrumentalist Theory of Propertisation'. *European Journal of Legal Studies*, 2010, 2, 3, The Future of... Law & Technology in the Information Society, p. 11, <http://cadmus.eui.eu/bitstream/handle/1814/15124/10_Property_EN.pdf?sequence=1>.

[189] See e.g. the *Mellacher* v. *Austria* case (1989), ECHR.

[190] Purtova, 'Property in Personal Data', p. 12.

[191] ibid., p. 17.

[192] Purtova, 'Private law solutions in European data protection', p. 16.

[193] P De Hert & S Gutwirth, 'Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence in the Institute for Prospective technological studies', *Security and Privacy for the citizen in the post-September 11 digital age: a Prospective overview*, 2003, cited in Purtova, 'Private law solutions in European data protection', p. 16.

requirement of consent[194] of a user of the social networking platforms.[195]

The ban on waiver of data protection rights means not a ban on voluntary exchange of personal information, but rather a prohibition of giving away for remuneration, among others, the right to consent. Therefore, commercial exchange of personal data is not, in principle, outlawed. However, treating data protection as nothing less than a fundamental right under Art. 8 ECHR will lift restrictions following from the fundamental right status[196] and will ban a full waiver of the right to data protection.

***

It is important to mention here, before we continue the legal analysis and proceed to the examination of the privacy-invasive practices of the SNSs, that the challenges that such practices predetermine are the result of implementation of an American view on personal data as on a property right (with a possibility to waive it on the basis of a contractual agreement), rather than a human right. This is quite understandable taking into account the fact that the majority and the most popular social networking platforms were created in the USA (including Facebook). Nevertheless, this mere fact of their birth under the American model shouldn't lead to a result of depriving the users, at least in Europe, of the means to protect their interests stemming from a recognition on the European level of a human rights nature of personal data. In other words, the creation of a property right in personal data and the possibility of its consequent waiver are not in line with the continental human rights-based approach to information privacy.

[194] Purtova, 'Private law solutions in European data protection', p. 16.

[195] See Subchapter 5.1.2., Chapter 5.

[196] Purtova, 'Private law solutions in European data protection', pp. 16-17.

5 The impact of Social Networking on the individual Right to Privacy in Data Protection: Challenges

It is probably impossible to identify and list all kinds of the information privacy risks arising in the area of social networking. Nevertheless, each of the risks emerges from the complexity of practical implications of one (or – more often – all) of the data protection principles, laid down, mainly, in the Data Protection Directive (though not only there, as the other European legal instruments are taken into account as well).

Accordingly, the first step in the analysis of this paper is to identify and characterize (though briefly) the named principles with the further aim to trace their implications in the context of social networking.

In accordance with this aim the second part of the current chapter's analysis will go into examination of the concrete and rather specific challenges of the SNSs, with a particular attention being given to one giant of the online world – Facebook.[197] As to be demonstrated, although diverse in nature, such challenges (as, e.g., behavioral advertising practices) flourish on the soil of violation and misuse of the general data protection principles.

The current chapter doesn't claim to concentrate on all of the data protection principles implemented on the European ground. Nevertheless, those under examination are: firstly, the most important for the purposes of the current research; secondly, in the most general way reflect the Privacy Directive's model approach to protecting the privacy interest of an individual in personal data; thirdly, have to be understood cumulatively, in a close link with each other, hence the breach of one principle, as to be demonstrated, often presupposes the breach of the other, and vice versa.

One more remark has to be done before we start the promised analysis. Though the current research is built around and stands for, mainly, the recognition of the Article 8 ECHR tools of protection of the individual's right to privacy in personal data, the way this human right is actually breached may be better examined on the basis of the norms and principles of the Data Protection Directive. Such approach is justified, to the author's opinion, by the previously demonstrated common nature of the privacy and data protection legislation and by the consequent view on them as on the two sides of one coin. It is to be shown that the profound and huge amount of privacy enhancing practices, currently existing in Europe in the area of

[197] Stoddart, 'Privacy in the era of social networking'.

social networking, amounts, if read cumulatively, to a level on which we can actually claim violation of the Article 8 ECHR right to privacy. The claimed violation is attributable (and it is to be proved, to a greater extent, in the last chapter of the current analysis) to the States that fail in fulfilling their positive obligations to regulate and protect the information privacy rights of the European citizens. Such failure is seen, from the one hand, in their inability to make the USA-originated social networking companies to abide to the already existing European privacy law (in the face, namely and mainly, of the Data Protection Directive), and, from the other, to implement the new laws in those spheres where the existing legislation turns to be insufficient and backward in regulating the relations in the new highly digitalized world, what makes the protection of Article 8 ECHR ineffective.

5.1 Basic principles of Personal Data Protection: Control, Consent and Transparency

The core principles chosen for the purposes of the current analysis are enshrined not only (though to a greater extent) in the Data Protection Directive, but also in a number of other instruments, including Council of Europe's Convention 108, the OECD's privacy guidelines, and etc.

Being representative of the legislative standards employed in Europe to protect an individual's privacy interest in personal data,[198] they may be formulated as the following:
(1) Enhancing control over one's own data (in a sense of establishing a set of obligations and responsibilities for the treatment of personal information);
(2) Ensuring informed, free and unambiguous consent;
(3) Increasing transparency for data subjects (closely linked, in turn, with the principles of purpose limitation and data minimization in collecting and processing personal data).

5.1.1 Enhancing control over one's own data

One of the key concepts of the European privacy protection legislation is that an individual should be in control over his or her personal information.[199] Privacy is all about freedom of choice and personal control over your personal information.[200]

---

[198] Gray, Hester & Cole, p. 5.

[199] ibid.

[200] A Cavoukian, 'When Online Gets Out of Line. Privacy: Make an Informed Online Choice', in *Information and Privacy Commissioner*, Ontario, 2006, p. 4, <http://www.ipc.on.ca/images/Resources/up-facebook_ipc.pdf>.

In the context of social networking the principle of an individual having control over his or her personal information goes on to delineate the type of information the SNS collects, why it collects the information, who has access to it and how to get rid of information.[201]

The main problem with the implementation of the principle of control is that whenever you put data on a computer, you already lose some control over it. And when you put it on the Internet, you lose a lot of control over it.[202] While some service providers have tried to create limited areas within their services to give users more control over their personal information, others provide less protection to such information or parts thereof available to a bigger audience, which may mean, in some cases, exposing the data to the entire community.[203] What providers are continuously trying to do is testing the new ways of exploiting the users' personal data; if they go too far, individuals complain. Via this push-and-pull process, providers and users are working out where the privacy line is.[204]

The system built on such self-regulation, together with the protection being dependant on the initiative (or lack thereof) of the companies to give users more or less control over their data doesn't seem to satisfy the threshold of protection which we expect to be granted to the fundamental human right, which privacy in personal information is.

In fact, there are at present only limited means to control information once it is putted on the SNS.[205] The scope of information dissemination, including personal data, on such web sites is unprecedented, as well as an access to such information. The authority over such information is so fragmented that the State loses control over data protection and the individual loses control, not only over the information, but also over any recourse in the event of a violation.[206]

---

[201] K E Martin, 'Case BRI-1 006 (A). Facebook(A): Beacon and Privacy', *Business Roundtable Institute for Corporate Ethics*, The Catholic University of America, 2010, p. 7, <http://www.darden.virginia.edu/corporate-ethics/pdf/Facebook%20_A_business_ethics-case_bri-1006a.pdf>.

[202] B Schneier, 'Facebook and Data Control'. *A blog covering security and security technology*, September 21, 2006, viewed on 6 May 2011, <http://www.schneier.com/blog/archives/2006/09/facebook_and_da.html>.

[203] International Working Group on Data Protection in Telecommunications, *Report and Guidance on Privacy in Social Network Services. "Rome Memorandum"*, 43rd meeting, 3-4 March 2008, Rome (Italy), pp. 5-6.

[204] M-R Roberson, 'Online Social Networks: Finding a Balance Between Sharing and Privacy', in *DukeToday*, 12 November 2010, viewed on 9 May 2011, <http://today.duke.edu/2010/11/cox.html>.

[205] *Report and Guidance on Privacy in Social Network Services*, pp. 1-4.

[206] C Bernier, 'Personal Data Protection Issues in a Globalized World. Remarks at the 3rd Conference of Francophonie Personal Data Protection and Privacy Commissioners', in *Office of the Privacy Commissioner of Canada*. Madrid, Spain, November 3, 2009, <http://www.priv.gc.ca/speech/2009/sp-d_20091103_cb_e.cfm>.

5.1.2 Ensuring informed, free and unambiguous consent and retention principle

Another basic principle of data protection imposes (in the majority of the situations) a ban on processing a user's personal data without that user's consent. The 1995 Data Protection Directive on which all EU national data protection legislation must be based defines "consent" as "any freely given specific and informed indication" of wishes signifying agreement to personal data being processed, and such consent must be given "unambiguously" (Article 7(a), Article 2(h)).[207] Consent must be obtained before the collection of personal data, as a necessary measure to ensure that individuals can fully appreciate that they are consenting and what they are consenting to. Furthermore, consent must be revocable,[208] which embraces the right to have the one's personal data rectified (data retention principle).[209]

The requirement of consent is also in line with Article 8 of the EU Charter,[210] as well as with the Article 5(3) of ePrivacy Directive.

The key challenge in the current SNSs dispute is deciding on the limits and forms of the consent, in other words, solving the problem of what would constitute informed, free and unambiguous consent to data processing.[211]

As to the issue of deletion of personal data, Article 6(1)(e) of the Data Protection Directive prohibits indefinite storage of personal information and requires its deletion when it is no longer necessary for the purpose for which

---

[207] Tavenerslaw.co.uk, 'Are social networks and European data privacy laws incompatible?' in *Taveners.*

[208] Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, adopted on 22 June 2010, 00909/10/EN, WP 171, p. 13, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf>.

[209] The possibility to withdraw consent serves yet as one more proof against treating personal data in the frameworks of contractual agreement. In the law of contracts consent is seen as a single transactional moment, while the data privacy legislation (and, what is notable, not only in Europe, but all around the world) looks at consent as at "an ongoing act of agency to the information subject". *See* J Barrigar, J Burkell & I Kerr, 'Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information'. *Canadian Business Law Journal*, vol. 44, pp. 56-60, <http://www.idtrail.org/files/LETS_NOT_GET_PSYCHED_OUT_OF_PRIVACY%20final%5B1%5D.pdf>.

[210] Tavenerslaw.co.uk, 'Are social networks and European data privacy laws incompatible?' in *Taveners.*

[211] European Commission, *A comprehensive approach on personal data protection in the European Union*, p. 8; J R Reidenberg & P M Schwartz, 'Data Protection Law and On-line Services: Regulatory Responses', *European Commission's Office of Official Publications*, Luxembourg, 1998, p. 8, <http://ec.europa.eu/justice/policies/privacy/docs/studies/regul_en.pdf>.

the data were collected (retention principle).[212] In the context of social networking Article 6(1)(e) may be interpreted to require:
(1) limiting the storage of information by means of setting express timeframes under which data will be retained by a particular SNS. The indefinite or overly long retention periods are, therefore, would be in contradiction with Article 6(1)(e) of the Directive.[213]
(2) deletion of personal information about the user of the SNS if it is no longer needed for the development of a profile (right to be forgotten).[214]

The problem of practical implementations of the principles of consent and data retention is discussed in more detail in the second part of this chapter during the course of analyzing the opt-out default privacy settings, together with the current policies of the social networking platforms in deleting the users' personal data.

5.1.3 Increasing transparency for data subjects and principles of purpose limitation and data minimization

The third key element in the European data protection principles is the maintenance of transparent processing systems for personal information. This means that processing activities must be structured in a way that makes them open and comprehensible, letting the individuals to be fully aware of the treatment of their personal data.[215]

The requirement of transparency presupposes, among others, the ways of collection and usage of personal data.[216] The European data protection framework with this regard is built generally on the two requirements:
(1) the collection of personal data is allowed only for specific purposes[217], and, being collected, such personal data can be used only for the purposes which are compatible with the stated purpose of collection[218] (purpose limitation principle);
(2) there are limits for the collection of excessive or unnecessary

---

[212] Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, p. 20.

[213] ibid.

[214] ibid.; V Reding, 'Why the EU needs new personal data protection rules', Speech 10/700 at the *European Data Protection and Privacy Conference*, Brussels, 30 November 2010, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700&format=HTML&aged=0&language=EN&guiLanguage=en>.

[215] Reidenberg & Schwartz, pp. 7-8.

[216] Le Bail, p. 4.

[217] European Convention 108, Art. 5(b); EU Data Protection Directive, Art. 6(b).

[218] European Convention 108, Art. 5(b); EU Data Protection Directive, Art. 6(b).

information[219] (principle of data minimization).[220]

Both of the principles of collection and usage may be claimed to fall within the scope of a broader principle of transparency, although they are closely linked and interacted with the principles of consent and, specially, control.

(1) **The purpose limitation principle** is enshrined into the Article 6(1)(b) of the Data Protection Directive**.** This principle (going in line also with Article 8(2) of the EU Charter) has a twofold aim: first, it prohibits the unjustified collection of personal data; secondly, it prohibits the processing of personal data, which is not compatible with the purposes that legitimized the initial collection (in other words, incompatible secondary uses of the information collected and stored would contradict the Data Protection Directive).[221] In the wording of the Data Protection Directive, it is required for personal data to be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with these purposes."[222]

(2) **The data minimization principle** restricts the collection and further processing of unnecessary personal information.[223] It is enshrined in the Article 6(1)(c) of the Data Protection Directive, which binds the State-signatories with obligation to ensure that personal data is “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.”

While this component does not offer specific guidance for determining whether particular piece of information is necessary for an identified collection purpose, the personal information collectors within Europe do not have unlimited discretion in this regard. Rather than trying to maximize the gathering of personal data, the companies must try to minimize it and collect only the least amount of personal information compatible with an intended purpose.[224]

In overall, transparent or open processing of personal information is the mechanism with the help of which an individual is able to exercise control over his or her personal information, as well as to express an informed consent[225] (e.g., in the absence of transparency, an individual's consent to the data processing practices of on-line social networks cannot be

[219] European Convention 108, Art. 5(c); EU Data Protection Directive, Art. 6(c).

[220] Gray, Hester & Cole, p. 6.

[221] Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, p. 20.

[222] Directive 95/46/EC, at Art. 6(1)(b).

[223] Reidenberg & Schwartz, p. 5.

[224] ibid., pp. 5-6.

[225] Gray, Hester & Cole, p. 7.

considered to be valid).[226] Therefore this principle is closely linked with the two discussed above.

Meanwhile, the growth in on-line services has not been accompanied by an increasing transparency for data subjects.[227] As the character of the current privacy policies and practices implemented by SNSs show, the users may not know or understand the technology that supports the social networking platforms. The question of whether sufficient and effective information is provided by SNSs in a way that will reach the users raises serious doubts.[228]

The practical implications of the principle of transparency and various challenges in this regard are illustrated in the second part of the current chapter on the examples, inter alia, of the SNSs' practices in collecting and processing of their users' personal data, behavioural advertising practices, and etc.

5.2 Specific challenges

Once placed on a SNS, the user's personal information is facing several threats touching upon the right to privacy. Though it is possible to delineate some risks associated with the provision and usage of such services already now, it is very likely that we are at present only looking at the tip of the iceberg, and that new uses – and accordingly new risks – will continue to emerge in the future.[229]

In order to limit what could otherwise have been a virtually limitless analysis, the paper sets out categories of activity common to social network sites, and proceeds to canvas the policy choices of some of the selected sites for each category. While this will not, of course, cover all the privacy implications endemic to each site, it does provide a platform for understanding privacy issues and the policy choices sites have made regarding those particular issues across the board.[230]

Accordingly, this subchapter, being built on the understanding of the three core data protection principles presented in the previous subchapter, goes to describe only the most "prominent" of the privacy dangers, placing them in the following categories:

---

[226] Reidenberg & Schwartz, p. 8.

[227] ibid.

[228] Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, pp. 13-15.

[229] *Report and Guidance on Privacy in Social Network Services*, p. 2.

[230] J Barrigar, 'Social Network Site Privacy: A Comparative Analysis of Six Sites', in *Office of the Privacy Commissioner of Canada*, February 2009, p. 3, <http://www.priv.gc.ca/information/pub/sub_comp_200901_e.cfm>.

(1) the SNSs' privacy policies. Default opt-out privacy settings (highly related to the implication of the principle of the user's informed consent);
(2) Collection of personal information;
(3) Sharing of user's information with third parties: behavioural advertising (which in itself raises a lot of privacy issues in the on-line environment and could be the topic of a separate research. Though, for the purposes of the current analyses, it will be narrowed to the data protection issues arising from the use of behavioural advertising mechanisms in the context and in the field of on-line social networking services, in particular, Facebook practices in this regard);
(4) Sharing of user's information with third parties: third-parties applications;
(5) Deletion of personal information from the SNSs.

The following list of risks, again, can only represent a snapshot, which may need to be revised and updated as social network services develop.[231] The author finds a comparison, given by Jennifer Stoddart, a privacy commissioner of Canada, as being of a particular relevance here. She draws the parallel between privacy challenges represented by SNSs and a classic arcade game – "whac-a-mole". "In that game, a mole pops his head up through a hole and you whack it with a rubber mallet. As fast as you can whack, however, another mole pops up in a different hole. Sometimes trying to respond to infringements of personal privacy by social networking and other online sites seems dangerously close to playing whac-a-mole."[232]

5.2.1 Privacy Policies: "Consent trap", opt-out default privacy settings and policy changing practices

A great majority of the SNSs currently operate under complex and over-lengthy privacy policies, that in the most cases creates difficulties in understanding for an ordinary user. Sometimes such policies are not even easy to find on a particular web-site. In addition to the complexity, a lot of SNSs implement confusing settings, use ambiguous wording in presence of inconsistent use of terminology between sections of the same site's privacy settings.[233] Besides, the policies are often changed by the companies without even informing the users.

The following issues, originating from or closely related to the problem of complexity of the SNS's privacy policies, are examined below.

(1) "Consent trap"
In line with an American view on personal information, privacy policies of

---

[231] *Report and Guidance on Privacy in Social Network Services*, p. 2.

[232] Stoddart, 'Privacy in the era of social networking'.

[233] Bonneau & Preibusch, pp. 21-23.

the SNSs understand the user's consent as merely an act of clicking through a "consent" screen on a Web site. This is seen by such SNSs as an exercise of a self-reliant choice, which leads into the "consent trap". It means that this screen contains a cliché language that permits all further processing and transmission of one's personal data. Even without a consent screen, some Web sites place consent clichés within a "privacy statement" on their home page or elsewhere on their site, usually having the following (or very similar) wording: "By using this site, you agree to its Privacy Policies." Such language presents the conditions for data processing on a take-it-or-leave-it basis. It seeks to create the legal fiction that all who visit the site have expressed informed consent to its data processing practices. An even more extreme manifestation of the "consent trap" is a belief that an initial decision to surf the web itself is a self-reliant choice to accept all further use of one's personal data generated by this activity. The reality is, however, that individuals can be trapped when such glorification of freedom of action neglects the actual conditions of choice.[234]

(2) Opt-out default privacy settings

The complexity of privacy policies makes the task of comprehending information, forming them, more difficult than it needs to be with a result of just a small percent of users actually reading and even less understanding it.[235]

In this light the following statistics are eloquent:
- less than 3% of SNSs' users read privacy policies;
- 75% of users think that the existence of a privacy policy implies privacy protection;
- 54% of privacy policies are beyond the grasp of 57% of the Internet population (requiring the equivalent of more than fourteen years of education);[236]
- a significant number of users are not even aware that privacy controls exist in social networks, estimated in two different studies at 26%[237] and 30%.[238]

One of the conclusions that may be derived from these statistics is that the issues of presentation and default settings in fact have a decisive influence on the individual's perceptions and choices when it comes to privacy.[239] In

---

[234] Solove, Rotenberg & Schwartz, p. 50.

[235] EPIC.org, 'Social Networking Privacy', in *Electronic Privacy Information Center*, viewed on 9 May 2011, <http://epic.org/privacy/socialnet/#back>.

[236] Acquisti, 'Awareness, Understanding, and Individual Decision-Making'.

[237] H Jones & J H Soltren. 'Facebook: Threats to privacy', 2005, <http://web.mit.edu/jsoltren/www/facebook.pdf>, cited in Bonneau & Preibusch, p. 18.

[238] A Acquisti & R Gross, 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook', in *Privacy Enhancing Technologies*, LNCS 4258, Springer Berlin / Heildelberg, 2006, pp. 36–58, cited in Bonneau & Preibusch, p. 18.

[239] OECD, *The Evolving Role of the Individual in Privacy Protection: 30 Years after the OECD Privacy Guidelines*, 32 International Conference of Data Protection and Privacy

other words, a great majority of users would simply agree with the privacy policies suggested to them by a social network provider being in place on the web site by the time of a user's registration (default privacy settings).

Currently the majority of SNSs providers, including Facebook, increasingly offer "opt-out" privacy mechanisms by default in their privacy policies, which they assume to represent a user's consent in the meaning of the Data Protection Directive.

Meanwhile, it seems not to be self-evident at all that such a consent by the way of opt-out options provided by SNSs meets the requirements of the Directive (Art. 7(a), Art.2(h)).[240]

By relying on the mechanism of an opt-out consent, the users, while signing up for a network, let the SNS preselect privacy settings that control an amount of a user's personal information accessible by others and, what is especially noteworthy for the current discussion, whether search engines (including Google) have an access to such information.[241] In doing this, the user actually enables sharing of certain amount of his or her personal information with anyone on the network by default. If users wish to change their privacy settings and limit the access to their private information, they have to go to the website and explicitly indicate their wish to opt-out. In spite of the fact that the settings can be customized by users to reflect individual preferences, if they do not do so, their private information will be made available from the start to the third parties.[242] As a result, such default settings put everyone at the weakest privacy level from the very start, making their personal information public.[243]

The main problem is in fact not the lack of options but the almost universality of open defaults. Though varying in the previous literature and depending on the site in question, but estimates demonstrate that between 80 and 99% of users are typically found to never change their privacy settings.[244] According to statistics, 90% of SNSs leave new profiles

---

Commissioners, Jerusalem, Israel, 25-28 October 2010, <http://www.oecd.org/document/44/0,3746,en_2649_34255_45780844_1_1_1_1,00.html>.

[240] Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, p. 15.

[241] E Denham, 'PIPEDA Case Summary #2009-008: Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act', in *Office of the Privacy Commissioner of Canada*. 2009, p.18, <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm>.

[242] ibid., p. 20.

[243] A Illmer, 'Data protection commissioner warns over social networking sites', in *DW-WORLD.DE Deutsche Welle*, 27 December 2009, viewed on 9 May 2011, <http://www.dw-world.de/dw/article/0,,5060457,00.html>.

[244] Acquisti & Gross, 'Imagined Communities', pp. 36–58; B Krishnamurthy & C E Wills, 'Characterizing Privacy in Online Social Networks', in WOSN: Workshop on Online Social Networks, 2008, pp. 37–42; cited in Bonneau & Preibusch, p. 18.

completely visible to at least all other members of the site by default.[245]

It seems that such opt-out mechanisms do not *per se* deliver the average users' informed consent. The reasons are, namely:

First, generally average users of SNSs are lacking the basic understanding of the ways in which the technology works and, what is more important, how to exercise the opt-out options in practice.[246] Privacy policies of a great majority of SNSs, again, are highly complicated and extremely long. According to BBC News, Facebook's privacy policy has 50 different setting possibilities and 170 alternative privacy options. In such circumstances Facebook may face the difficulties in showing that it provides for an *informed, free and unambiguous consent*.[247]

What goes as a consequence is that practically an opt-out option is exercised by a small number of users, not by the reason of making an informed and free decision to accept the default privacy settings suggested by the web-site, but rather due to the fact of not being fully aware that by the way of not exercising they are actually consenting.[248] This being so in the circumstances when only 20% to 30% of users, according to Facebook estimations, change their privacy settings. In the case of Facebook, it does not inform its users that failure to change the default settings constitutes consent to those settings.[249]

Second, consent presupposes an active participation of an individual prior to the collection and processing of his or her personal data, while an opt-out option often refers to a "non"-action from the side of an individual and is exercised after the processing has already started. There is no active participation under an opt-out option. The will of an individual is simply and basically assumed or implied, which doesn't meet the requirements for legally effective and especially unambiguous consent.[250]

Third, it follows from the legislative requirement of unambiguous consent that it must be clear to individual what he or she is consenting to. Therefore when privacy policy states, for example, that the company "also shares information with other carefully selected third parties" (what is quite often the case with behavioural advertising or the third parties' applications), it

---

[245] Bonneau & Preibusch, p. 18.

[246] Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, p. 15.

[247] Tavenerslaw.co.uk, 'Are social networks and European data privacy laws incompatible?' in *Taveners.*

[248] Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, p. 15.

[249] Denham, p. 19.

[250] Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, pp. 15-16.

remains totally unclear what you are giving your consent to.[251]

With individual not being fully aware with what he or she is consenting while signing for the SNSs service, a personal data can't be regarded as being protected and the requirements of the Data Protection Directive fail to be fulfilled with the broader consequences of putting into danger the right to privacy as safeguarded, inter alia, by Articles 7 and 8 of the EU Charter.[252]

So long as Facebook, along with the other social network providers, bases its privacy policies on the opt-out default settings, it will continue to put its users at the risk and will play a dangerous role in degrading a fundamental human right that is the right to privacy.[253]

(3) Policy changing practices

Another related problem is that the SNSs frequently change their privacy policies or reset users' privacy preferences, putting them back at the default level.[254] This often happens without appropriate users' notification, let alone their consent, in contradiction of Articles 6(a) and 7(a) of the Data Protection Directive. This was the case, for example, when Facebook without any warning changed the rules on distribution of its users' personal information. It happened in 2006 when the company introduced a new feature called "News Feeds" combining and showing all kinds of actions the users do on the site.[255] These changes were presented to the users automatically. Consequently, one of the users' and privacy advocates main concerns was that individuals were not explicitly told how the News Feed feature worked and what were the privacy options in this regard.[256] Millions of members have originally putted their personal information on the site based on a set of rules about how that information would be used and all of a sudden these rules changed,[257] without any acknowledgement from the side of Facebook that the aggregation of information allows for presentation of data in a highly digestible form, which raises privacy concerns in the

---

[251] J Kohnstamm, 'New European Rules on Data Protection?' Speech at *Joint High Level Meeting on Data Protection Day*, 28 January 2010, <http://www.data-protection-day.net/files/Panel_1_4_Jacob_Kohnstamm_Speech_OK_for_website.pdf>.

[252] Denham, pp. 24-25.

[253] M Roggensack, 'Facebook Confuses "Security" and "Privacy"', in *Human Rights First*, 28 January 2011, viewed on 9 May 2011, <http://www.humanrightsfirst.org/2011/01/28/facebook-confuses-"security"-and-"privacy"/>.

[254] EPIC.org, 'Social Networking Privacy', in *Electronic Privacy Information Center*.

[255] Schneier.

[256] Privacy International, 'Social Network Sites and Virtual Communities', in *Privacy International*, 18 December 2007, viewed on 9 May 2011, <https://www.privacyinternational.org/article/phr2006-privacy-topics-social-network-sites-and-virtual-communities>.

[257] Schneier.

sense, *inter alia*, of the principle of consent.[258]

Another example illustrating how the principle of consent can be overstepped by on-line social networking giants (by simply using the default privacy settings) is the introduction by Google in February, 2010, of a new social network service called "Buzz" to the accounts of the 146 million users of its free Gmail service. The default settings initially revealed (in the network of "followers") the people with whom Gmail users e-mailed and chatted most,[259] without adequately informing those users about how this new service would work or providing sufficient information to permit informed consent.[260] This actually ended in the unpermitted disclosure of the users' personal information. What followed was an immediate and vociferous storm of protest from the Gmail community around the world. Within days, Google quickly apologized and introduced changes to address the widespread criticism.[261]

Both of the cases with Facebook's News Feed and Google's Buzz demonstrate a highly dangerous tendency of on-line social network providers to roll out a product that unilaterally renders personal information public with the intention of repairing problems later as they arise.[262] As was expressed by the journalist in one of the interviews with the CEO of Facebook broadcasted on-line, "Facebook doesn't ask for permission, it asks for forgiveness".

It's quite obvious that such kind of approach in dealing with private information of the users of SNSs completely undermines the whole idea behind the respect for the right to privacy as a fundamental human right. Not mentioning that this practice goes against the requirements of Article 5(3) of ePrivacy Directive, which places a special stress on the provision of prior information and obtaining prior consent before the processing of personal data starts.

All of these being said makes the questions of adherence by SNSs in their privacy policies to the principles of control, consent and transparency highly controversial.

5.2.2 Collection of personal information

The SNSs' privacy-enhancing practices in collecting the users' personal information are examined here in the light of the data collection principles (purpose limitation and data minimization), already described above within

---

[258] Privacy International, 'Social Network Sites and Virtual Communities'.

[259] Stoddart, 'Privacy in the era of social networking'.

[260] Stoddart, 'Why Privacy Still Matters'.

[261] ibid.

[262] Stoddart, 'Privacy in the era of social networking'.

the framework of the principle of transparency.

(1) The purpose limitation principle
As the current practices demonstrate, the basic principle of purpose limitation in collection of personal information has become the exception rather than the rule in the on-line environment.[263]

As a registration condition Facebook requires all users to provide their full name, email address, desired password, gender and a real date of birth. With regard to the last requirement the company does not adequately explain to users why they have to provide their dates of birth and how these would be used, in contravention of the purpose limitation principle.[264] The only explanation, which Facebook gives is that it "do this as a safety precaution and to help ensure that the site is useful for people."

It is important to stress that Art 6(b) of the Data Protection Directive stipulates that purposes must be not only legitimate, but also explicitly specified. It is quite questionable whether the above phrase used by the website to reflect the purpose of collection corresponds to the requirement of an explicit specification. On the opposite, the purpose statement as explained in the cited phrase is rather vague and indefinite. Besides, the phrase is not clear enough to ensure also that users have the knowledge for making an informed choice about consent under Art 7(a) of the Data Protection Directive.[265]

Moreover, Facebook does not specify the other purposes for which it collects the dates of birth of its users – namely, targeted advertising in accordance with the age. Therefore, the site at the time of registration doesn't notify its users about all the purposes for which it collects and uses the dates of birth of individuals. Although the Privacy Policy does discuss in general terms the purposes for which "profile" information may be used, including purposes of targeting advertising, it does not refer to dates of birth specifically in that context, while (in order to comply with the Data Protection Directive's requirements) it should be distinguished and its uses specifically explained in the Privacy Policy.[266]

(2) Data minimization principle
An on-line environment also threatens the requirement imposing the ban on collection of unnecessary personal information.[267] In general, far more personal data are collected than is needed for a user to interact with a social networking service, particularly gender and date of birth information.[268]

---

[263] Reidenberg & Schwartz, p. 5.

[264] Denham, p. 10.

[265] ibid., p. 15.

[266] ibid., p. 15.

[267] Reidenberg & Schwartz, p. 6.

[268] Bonneau & Preibusch, p. 15.

The results of a Cambridge University study illustrate the tendency towards maximization in collecting data about users. The study has shown that almost 90% of the SNSs needlessly require a full name or date of birth for permission to join. Gender was required by 20 sites (out of 29) and requested by 4 others. A full date of birth was required by 24 sites and requested by 2 others.[269]

These two pieces of data are both useful to personalize the site but should not be mandatory.[270]

Within the problem of collection by the SNSs of excessive information about their users also fall the requirements to provide the other kinds of personal data. For example, the SNS BlackPlanet mandatory requests a user's race, ancestry, income level, and sexual orientation during the process of signing up.[271]

It is also remarkable that every site, according to evaluation, requires an individual to provide his or her email address in order to join. Although it is easy to obtain free and disposable email addresses online, most users will enter their real email addresses, making the insistence on providing of such information a needless privacy violation since it is not necessary for an interaction with the social networking platforms.[272]

5.2.3 Targeted advertising

Another area in the realm of social networking, raising important data protection and privacy related concerns, is targeted advertising and its role in disclosing of users' private information to the third parties.[273] It is closely linked to the risks the complexity of SNSs privacy policies gives rise to.

Behavioural advertising is defined as a marketing practice of targeting advertisements to users on the basis of observed or known personal characteristics, such as age, profile and online activity; it therefore entails the collection and retention over time of personal data and it involves consumer tracking. The personal information collected may include IP address, pages visited, length of time spent on pages, purchases etc. Besides, it tracks a pattern of on-line activities.[274] Online advertising is a key source of income for a wide range of online services and is an important factor in

---

[269] ibid.

[270] ibid.

[271] ibid.

[272] ibid., p. 17.

[273] Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, p. 4.

[274] ibid., pp. 4-5.

the growth and expansion of the Internet economy.[275]

Clearly, it is necessary to enter some personal information if one wishes to participate in a social networking website. However, there are large amounts of additional disclosure (primarily to advertisers) going on.[276] The relevant provisions on the information to be given to the data subject about targeted advertising practices are not sufficient, challenging the principles of control and informed consent.[277]

Thus, the privacy features of Facebook allow for virtually no controls on what the company can expose to advertisers. The blanket statement regarding disclosure allows Facebook to provide almost any personal data to advertisers. It also allows advertisers to set cookies that are not governed by the privacy policy. [278]

In the light of a controversial nature of behavioural advertising it is possible to highlight two potential problems.

First is the problem of anonymity. The majority of SNSs rely on anonymity in the context of targeted advertising as on the basis for justification of their practices under the data protection laws. The advertising and analytics industries have traditionally claimed that their activities fall outside the scope of privacy legislation because they only collect and use anonymized data. However, there is also a growing body of research showing how easily data that is thought to be anonymous can be re-identified.[279]

The case is that some providers of social networking services fail to clearly communicate the fact that they transmit their users' IP addresses to advertising companies, assuming that IP addresses are not personal data. Meanwhile the current technologies make it possible to associate a user's IP with his or her personal information including name, address, and telephone number.[280] As a result, a user's personal data are disclosed to the third party without that user's consent and even knowledge about it.

This brings us to the second problem, which is consent. In most cases, individuals are simply unaware about targeted advertising. Information

---

[275] D S Evans, 'The Online Advertising Industry: Economics, Evolution, and Privacy', University College London and University of Chicago, April 2009, p. 2, <http://www.intertic.org/Policy%20Papers/EvansEOAI.pdf>; 'Online Behavioural Advertising', in *Office of the Information and Data Protection Commissioner*, <http://idpc.gov.mt/dbfile.aspx/Behavioural_advertising.pdf>.

[276] H Jones & J H Soltren, *Facebook: Threats to Privacy*, 14 December 2005, p. 23, <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf>.

[277] – European Commission, *A comprehensive approach on personal data protection in the European Union*, p. 6.

[278] Jones & Soltren, p. 24.

[279] Bernier, 'Online Behavioral Advertising'.

[280] ibid.

SNSs provide to their users about targeted advertising often fall short of the requirements of data protection legislation.[281] This stretches the notion of consent: choosing to target a user for advertising assumes a level of receptiveness, or consent about the use of personal information, that may simply not be there.[282] Both the proliferation of actors involved in the provision of behavioural advertising and the technological complexity of the practice make it difficult for an individual to know and understand if personal data are being collected, by whom, and for what purpose.[283]

A recent case with Facebook serves as a good illustration of the outlined privacy problems. On November 2007 the company began offering a free tool, Beacon, to a number of its online partners (such as Blockbuster, The New York Times, and Overstock.com) for tracking the users' activities.[284]

Residing on a partner's website, the Beacon program captured detailed data along with IP addresses of all visitors on a partner site—Facebook users and non-Facebook users—and (if it identified a visitor as a Facebook user) proactively broadcasted such off-Facebook activities on Facebook, making the information available to the user's friends through an existing service called News Feed. Meanwhile Facebook's attempts to inform its users of this new feature were highly questionable. Users were not given the ability to reject all sharing. They were not informed that data on their activities were always flowing back to Facebook, nor given the option to block that information from arriving at Facebook.[285]

Due to a huge privacy-related uproar caused by the feature, Facebook was forced to close it just in a month after its introduction on the market, but the Beacon case illustrated once again how the company overstepped the principles of control, consent and transparency in disclosing the information about its users' without their explicit permission.

5.2.4 Sharing of personal data with third parties' apps

Another way to make the users' data available to third parties, which is also broadly practiced by the SNSs, is disclosure of such data via application

---

[281] Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, p. 11.

[282] Bernier, 'Online Behavioral Advertising'.

[283] European Commission, *A comprehensive approach on personal data protection in the European Union*, p. 6.

[284] K Martin, 'Facebook (A): Beacon and Privacy', *Business Roundtable Institute for Corporate Ethics*, 2010, p. 2, <http://www.darden.virginia.edu/corporate-ethics/pdf/Facebook%20_A_business_ethics-case_bri-1006a.pdf>.

[285] ibid.

programming interfaces.[286] Very often SNSs allow the third-party software programmes ('apps') to access the users' data.[287]

In the light of the impact of apps on the right to privacy the following matters raise serious concerns:

(1) In practise the SNSs (including Facebook) give third-party application developers potentially unlimited access to the users' information.[288] When users add an application, they must consent to allow the third-party application developer to have access to their personal information, as well as that of their friends. Moreover, unless users completely opt out of all applications and block specific applications, they are not given the option of refusing to share their names, networks, or lists of friends when friends add applications.[289]

It seems that to make all of a user's personal information accessible to a third party is in effect to disclose it to that party. It doesn't appear to be appropriate, especially given that the third party would typically need very little of the information for its own purposes.[290] Such an unlimited disclosure of the users' personal information to the third parties by means of apps raises serious concerns with regard to the principles of data minimization and purpose limitation.

(2) Again touching upon the question of consent, it is usually sought in the most formal sense (i.e. "give consent or you cannot use the app"), but usually an individual has to give away all of his or her personal data on the SNS or not be able to access the platform at all.[291]

Facebook's manner of seeking consent raises questions here in two ways. First, Facebook operates with an excessively broad consent language.[292] Second, no specific consent is sought from users for the disclosure of their personal information to applications when their friends and fellow network members add applications. The only way users can control the exposure of their personal information to application developers when their friends and fellow network members add applications is either to opt out of all applications altogether or to block specific applications. Moreover, the latter

---

[286] *Report and Guidance on Privacy in Social Network Services*, p. 3.

[287] Since May 2007, Facebook has provided third parties with a platform (Facebook Platform) that enables them to create within Facebook applications that users can add to their accounts. These applications, which include such items as games, quizzes, horoscopes, and classified ads, access Facebook's database, but reside on the developers' servers. *See* Denham, p. 38.

[288] Denham, p. 48.

[289] ibid., p. 38.

[290] ibid., p. 51.

[291] ibid., p. 53.

[292] ibid., p. 52.

option would effectively require them to guess which of the more than 350,000 applications their friends and fellow network members are likely to add.[293]

Therefore, Facebook operates in contravention of the Data Protection Directive requirements in that it does not provide for users' informed and unambiguous consent to the disclosure of their personal information to application developers when either the users themselves or their friends and networks add applications.[294]

5.2.5 Storage and deletion of personal information (right to be forgotten)

As have been shown, personal data can easily be stored and then even more easily multiplied on the Web. But it is not easy to wipe it out.[295] The notion of oblivion does not exist on the Internet.[296] The mere fact is that the Internet never seems to forget.[297]

Once published on the SNS, data may stay there literally forever - even when the data subject has deleted them from the "original" site, some service providers refuse to speedily comply (or even to comply at all) with the user's requests to have data, and especially complete profiles, deleted.[298]

Meanwhile the basic structure of data protection imposes obligations on the treatment of personal information once collected. A critical component places limits on the duration of storage of personal information. Any collection of personal information will lose accuracy and relevancy with time; as a result, organizations are not permitted to warehouse personal data for unlimited periods.[299]

Bearing in mind a described above principle of data retention (Article 6(1)(e) of the Data Protection Directive), the following must be said.

Facebook's initial approach to the deletion of personal data about the users of the site was quite problematic. From the beginning the company had been offering only the option of account deactivation. It meant hiding a user's profile from public view, but not deleting it as such, since the information

---

[293] ibid., p. 53.

[294] ibid., p. 53.

[295] Reding.

[296] *Report and Guidance on Privacy in Social Network Services*, p. 2.

[297] J Rosen, 'The Web Means the End of Forgetting', *The New York Times*, 21 July 2010, p. 1, <http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html>.

[298] *Report and Guidance on Privacy in Social Network Services*, p. 2.

[299] Reidenberg & Schwartz, p. 6.

still had been kept on Facebook's servers.

This original approach was changed by the company in February 2008. From that date Facebook started allowing its users an option of a permanent account deletion by means of directly contacting Facebook and expressing a wish to have their account rectified (with an alternative option of account deactivation still being in place and available for users).[300]

However, several problems with implementation of a retention principle remained in place even after this change in the company's policy, raising serious concerns on the point of invasion of one's privacy. They are the following.

Firstly, options of (permanent) account deletion and (temporary) account deactivation are neither currently made equally available to users, nor they are clearly distinguished from each other with an effect of indefinite retention of its users' information by Facebook. Though both options can be exercised by users (by referring to the Help section on Facebook), they are not given an equal exposure: only the option of account deactivation is currently included into Account Settings page. This may cause some users to assume that account deactivation is the only option available to them. Even more concerns raises the fact that the company does not explain the account deletion and account deactivation options in its Privacy Policy, though it seems reasonable to say that privacy-related matters should be explained in the organization's privacy policy, regardless of where else they may be explained.[301]

Secondly, the account deactivation option doesn't include a specified retention period, nor does it allow the user to set a period after which the information will be deleted from Facebook's records, as Article 6(1)(e) of the Directive demands.[302]

Such indefinite retention of users' personal information in deactivated accounts by Facebook, therefore, goes as well in contravention with Article 6(1)(e) of the Directive. While it is true that by deactivating their accounts users are in effect choosing to have Facebook temporarily retain unused personal information, it seems inappropriate (following the retention principle) for Facebook to continue to retain indefinitely the personal information of a user who has not reactivated an account for a long time. The longer an account remains deactivated and the information in it unused, the more difficult it is to argue that retention of the user's personal information is reasonable for the social networking purposes for which it was collected.[303]

---

[300] Barrigar, 'Social Network Site Privacy', p. 11.

[301] Denham, p. 62.

[302] ibid.

[303] ibid.

Thirdly, Facebook stresses itself that deletion of data is technically challenging and that it is impossible to completely delete all information from the site.[304]

All the above observations show that the current legislation, apart from not being followed by the social networking companies, is additionally in need for clarification of, inter alia, the so-called 'right to be forgotten', meaning the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes.[305]

***

What may be concluded from the given analysis of a vast amount of the SNSs-related privacy challenges, is that, apart from the legislation being in need of revision, the SNSs operating in Europe do not abide to even this, "out of digital age fashion" legislation.

Due to its nature and purpose, the current paper doesn't go into the discourse of a necessity of the revision of European privacy legislation. The European legislative community has already started and made a good progress in this direction with a substantive legislative reviews and amendments being expected this year (2011). Without any doubt, such developments are of an importance that can't be overestimated. They are for sure needed to reflect upon a changed nature of the digital space. But, into what this paper does go, is acknowledging the fact that the way social networking business currently operates in Europe doesn't stand the test even of this "old-fashioned" legislation.

In particular, a number of Facebook practices, as has been demonstrated, violate the requirements of the Data Protection Directive.

This situation can be explained (but not justified) by the fact that the majority of the SNSs (or at least the most popular ones with millions of active users) have emerged under the USA model of privacy, which treats personal data not as a part of a fundamental right to privacy, but rather as a property right, a commodity, which can be traded on a digital market in exchange for the free services it provides.

Meanwhile, Europe, as has been demonstrated previously, doesn't look at privacy in this manner. It grants personal data a level of protection no less than of a human right.

The problem is nevertheless that although the European present-day legal system doesn't recognize a property right in personal data, this is in no way

---

[304] ibid., p. 59.

[305] European Commission, *A comprehensive approach on personal data protection in the European Union*, p. 8.

mirrored in the practice of the on-line world.[306]

Therefore, an obvious result follows when the social networking business, created under one model, comes into the environment, which appeared and developed under a different model. Such result is a clash between the contractual nature of the SNSs' privacy policies and the right to the protection of personal data as guaranteed under the umbrella of Article 8 ECHR and (as a self-standing human right) – under Article 8 of the EU Charter, now having a binding effect on the Member States.

The main challenge currently is to balance between the right to privacy as guaranteed by Article 8 ECHR and the current situation of a rapid technological expansion.[307]

Clearly we have to find tools to help us to meet this one major challenge producing all those specific challenges analysed above. One of the tools, and the one for which the current research argues, already exists under the Article 8 ECHR. Though elaborated in the following chapter, in short it may be described as a further development of the concept of positive obligations of the States under Article 8 ECHR and recognition of a horizontal effect of the named Article on the relationships between private parties – in our case, between the social networking companies and the private users of the platforms. This would mean having a legal justification for the ban of waiver of the fundamental right to privacy on the ground of freedom of contract.

The task of the practical implementation of this tool is by no means demanding and will require States not only to implement privacy protective legislation, reflecting on the human rights nature of data protection, but also to ensure effective enforcement of such legislation, specially a compliance with it by the companies, coming from the other side of Atlantic and providing their services on the European ground.

This task reflects the diversity and complexity of the 21st century[308] and the author prefers to leave it to legislators and politicians. As the current research doesn't bear the nature of a legal draft for a proposed privacy legislation, it nevertheless suggests the grounds on which this legislation can be built or, in other words, directions in which the laws that are already in place in Europe may be interpreted, and in which the case law of the ECtHR may (and already have started to) develop.

---

[306] Prins, pp. 5-7.

[307] Jagland, p. 14.

[308] ibid., p. 15.

6 How to protect the right to privacy on the SNSs in Europe? Article 8 ECHR; Four lines of cases

It has already been shown that the scope of the right to privacy under Article 8 ECHR goes beyond protection of secret personal information and also regulates the use of collected data, arguing that in the system of the ECHR data protection interests are treated under the umbrella of Article 8 right to privacy. Therefore, it's been proved that data protection is an integral part of the human right to privacy as protected by the ECHR,[309] and, consequently, can't be waived freely on the contractual basis.[310]

As a next (and final) step in the legal analysis, the current chapter proceeds to rule that Article 8 ECHR also implies affirmative, or positive, obligations of a State with regard to the protection of personal data of the SNSs' users.[311] Furthermore, the issue of applying fundamental rights horizontally is addressed, i.e. whether, given the necessity to ensure the SNSs users' appropriate protection, the fundamental right to privacy may be invoked against private parties, especially taking into account that such parties are often registered (as a private business) outside of the European borders.[312] It will be proved that this is in fact legally justified by a dynamic interpretation of the Convention.[313]

The following analysis is built in four steps and deals accordingly with the four lines of the ECHR case law. The timing of the cases in relation to the subject under consideration is noteworthy: the lines of the cases follow the historical development of the Court's jurisprudence, reflecting it changes in accordance with the demands of a new digital society. In short, the argumentation is constructed as the following:

1. The first line of cases observes how the concept of positive obligations appeared in the Court's jurisprudence and developed through time in

---

[309] Purtova, 'Private law solutions in European data protection', p. 3.

[310] See Chapter 4, Subchapter 4.4.

[311] Purtova, 'Private law solutions in European data protection', p. 8.

[312] F Nawrot, K Syska & P Świtalski, 'Horizontal application of fundamental rights: Right to Privacy on the Internet', *9th Annual European Constitutionalism Seminar*, University of Warsaw, May 2010, p. 3, <http://en.zpc.wpia.uw.edu.pl/wp-content/uploads/2010/04/9_Horizontal_Application_of_Fundamental_Rights.pdf>.

[313] A Clapham, *Human Rights in the Private Sphere*, Clarendon Press Oxford, 1993, p. 98, <http://classes.lls.edu/fall2006/intlhumanrgts-romano/documents/HumanrightsClapham.pdf>.

general and within the scope of Article 8 in particular (based on the principle of "effectiveness" of enjoyment of Convention's rights). At this time and on this, first, level of the Court's case law an effect of positive obligations wasn't yet extended to the relationships between private parties.

2. In the second line of cases positive obligations of the States are derived from their responsibility to "protect" Convention rights, by protecting persons' rights from the acts of other private parties. In other words, the Convention's protection in this line of cases is extended to the sphere of the relations of individuals between themselves.

3. The third line brings data protection within the scope of Article 8 positive obligations. It calls, together with the second line of cases, for recognition of a so-called "indirect horizontal application" of the data protection rules within the scope of Article 8 right to privacy.

4. The fourth line of cases, finally, demonstrates the potential and possibilities of applying the concept of indirect horizontal effect of the ECHR on the relationships between European users of the social networking services from one hand, and private corporations, providing such services in Europe, but registered outside of the European borders – from the other (namely, in the USA, since, as have been mentioned several times before, this is the country from where the majority of the most popular SNSs have come to Europe, together with their "privacy as a commodity" model). The question of jurisdiction of multinational corporations will be touched upon under the heading of this fourth line of argumentation as well. It obviously can't be avoided while considering application of the norms of a European treaty to the parties providing their services from the non-European ground. However, as to be proved further, in so far as these private actors provide their services in Europe, they are subjected to the European jurisdiction, and the norms of ECHR apply to them (indirectly). One more important clarification: the author doesn't claim here that these corporations as such may be held responsible for the breach of the Convention's norms. As we are looking at "indirect" horizontal effect of the ECHR (Art. 8), those that may be held responsible are still the State parties to the Convention. But the reasoning behind finding them in violation of Art. 8 would be the breach of their positive obligations to protect the rights of the persons under their jurisdiction from violation originating in acts of the companies such as Facebook.

The analysis starts, therefore, with observing (briefly) the development of the ECHR case law on the States' positive obligations in general and with regard to privacy in particular, and, finally, narrows the scope to the context of the States' positive obligations to protect privacy in personal data.

6.1 The first line of cases

The idea of positive obligations was first brought up by the Strasbourg

Court in the *Belgian linguistic case*[314] In a more straightforward manner the concept was further developed in the cases of *Marckx* v. *Belgium*[315] and *Airey* v. *Ireland,*[316] the both of them concerning Art. 8 ECHR.[317]

As far back as the *Marckx* v. *Belgium* judgment, the Court inferred from the term "respect", as used in the first paragraph of Article 8, that it places positive obligations on the States inherent in an "effective respect" for family life in addition to the duty of non-interference in private and family life.[318]

In the *Airey case* the same approach was used in establishing positive obligations under Article 8 ECHR. The Court went to state: "The Convention is intended to guarantee not rights that are theoretical or illusory but rights that are practical and effective."

Thus, the Court has justified its findings of positive obligations in this first line of cases by the principle of effective enjoyment of rights. In other words, positive obligations were found to be necessary to make a Convention right effective.

One more case, based on the effective enjoyment principle and being of a particular interest for the current research, may serve as an illustration of the Court's reasoning under the first line of the case-law.

The case of *Gaskin* v. *UK*[319] concerned accumulated records of Mr. Gaskin's childhood dated back to the time when he was taken into care by the welfare authorities.[320] On the request of the applicant to access information the authorities answered by refusal to disclose the records. The last was justified by them on the ground of a necessity to protect confidentiality of contributors of the information. While recognising the legitimacy of the aim pursued by the welfare authorities, the Court, nevertheless, came to conclude that respect for private life "requires that everyone should be able to establish details of their identity as individual human beings." Accordingly, the Court decided that the failure of the State to set up procedures whereby the files could be available to the applicant constituted a violation of a positive obligation of the State under Article

---

[314] ECHR 23 July 1968 *'Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium'* v. *Belgium*, Applications no. 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64.

[315] ECHR 21 April 1979, *Marckx* v. *Belgium*, Application no. 6833/74.

[316] ECHR 9 October 1979, *Airey* v. *Ireland,* Application no. 6289/73.

[317] Nawrot, Syska & Świtalski, p. 16.

[318] J-F Akandji-Kombe, *Positive obligations under the European Convention on Human Rights. A guide to the implementation of the European Convention on Human Rights*, Human rights handbooks, No. 7, Council of Europe, 2007, p. 36.

[319] ECHR 7 July 1989, *Gaskin* v. *UK*, Application no. 10454/83.

[320] Akandji-Kombe, p. 38.

8.[321]

Thus, the Court confirmed by its ruling in the Gaskin case the obligation of the State to take steps to make sure that the enjoyment of the Convention right is effective.[322]

Based on the principle of effective enjoyment of rights, Article 8 ECHR jurisprudence has then evolved further[323] to make violations of the Convention's rights by private parties attributable to States (to compare: in the Gaskin case the violation of the applicant's right originated, strictly speaking, in the State's actions in the face of its public organs – the welfare authorities).

6.2 The second line of cases

In the second line of cases positive obligations are derived from the responsibility of the State Parties to "protect" Convention rights, by protecting persons' rights from the acts of others.[324] In other words, in this line of cases the decisions have been interpreted to support a claim that a State is obliged to ensure that the right is not interfered with even in the sphere of the relations of individuals between themselves, *i.e.* respected by private persons.[325]

The first clear indication of this came in *X and Y* v. *the Netherlands.*[326]

In this case the State was found in violation of Art. 8 ECHR for the reason of its criminal law not providing a means by which a sexual assault upon a mentally handicapped girl could be the subject to start criminal proceedings. According to the Court, Article 8 obligation to respect an individual's privacy imposed positive obligations that «may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves».[327]

The case of *X and Y* v. *the Netherlands* have revolutionized the ECHR privacy jurisprudence[328] and been labeled as a "landmark", highlighting "the importance of security measures in the protection of personal data in a

---

[321] Purtova, 'Private law solutions in European data protection', p. 9.

[322] ibid.

[323] ibid.

[324] D J Harris, M O'Boyle & C Warbrick, *Law of the European Convention on Human Rights*, Oxford University Press, New York, 2009, p. 19.

[325] Purtova, 'Private law solutions in European data protection', p. 9.

[326] Harris, O'Boyle & Warbrick, pp. 19-20.

[327] ibid., p. 20.

[328] ibid., p. 10.

manner that ought not to leave any uncertainties at least for the governmental actors."[329] The Court's judgment in the *X and Y* case suggests that the question is no longer: do the Convention rights apply in the private sphere? Now it is rather: to what extent do they apply?[330]

Another case that may be referred to the second type is the case of *Niemitz* v. *Germany.*[331] In the named case the Court extended the right to respect for private life to professional and business sphere, thereby rendering contractual arrangements between employer and employees invalid to the extent they are inconsistent with the right to privacy under Article 8 (the case concerned monitoring of an employee's email and surfing activities, that have been found to violate an individual's right to privacy in personal information).[332]

More recently, the Court has found positive obligations to protect individuals from invasions of their privacy in, inter alia, *Von Hannover* v. *Germany* judgment.[333] It has been ruled in this case that it is incumbent on the States to "ensure that the right of persons under their jurisdiction to their image is respected by third parties, including journalists."[334] The case concerned the Princess Caroline, a member of Monaco's ruling family. The photographs containing details of her private life were published in German press without her knowledge or consent. The Court found that the German state ought to clarify its legislation regarding the privacy of public figures[335] and emphasised the fundamental importance of protecting private life from the point of view of the development of every human being's personality.[336]

This trend (reflected in all of the above mentioned cases of the second line) towards extending the scope of the Convention to private relationships between individuals is known as an indirect horizontal effect of the Convention.[337]

It is important to clarify here that the mere fact that an individual has infringed a provision of the Convention cannot lead to a finding against the

---

[329] J Råman, 'European Court of Human Rights: Failure to take effective information security measures to protect sensitive personal data violates right to privacy – *I* v. *Finland*, no. 20511/03, 17 July 2008', *Computer Law & Security Report 24*, 2008, cited in Purtova, 'Private law solutions in European data protection', p. 10.

[330] Clapham, p. 90.

[331] ECHR 16 December 1992, *Niemitz* v. *Germany*, Application no. 13710/88.

[332] Bergkamp.

[333] ECHR 24 June 2004, *Von Hannover* v. *Germany*, Application no. 59320/00.

[334] Akandji-Kombe, p. 39.

[335] Nawrot, Syska & Świtalski, p. 16.

[336] Akandji-Kombe, p. 40.

[337] ibid., p. 14.

State. It is necessary for the conduct of the private individual to be seen as originating in a failing on the part of the State itself or as tolerated by it. In practical terms, it is because the State has been unable legally or materially to prevent the violation of the right by individuals, and otherwise because it has not made it possible for the perpetrators to be punished, that it risks being held responsible by the European Court. That finding is therefore justified as a general rule by a failure on the part of the State: what is held against it is that it has not taken steps.[338] In other words, the private entity's infringing act has to be regarded as originating from the State's failure to sufficiently protect given basic right,[339] i.e. it would not have occurred if appropriate legislation was in force.[340]

6.3 The third line of cases

Now, turning to the third line of cases, it must be said that it is of a particular interest for the current research since it brings data processing in private sector into the scope of Article 8 ECHR.[341] Besides, following the direction established by the Court in the previous two lines of its case law, the third line of cases became a real death stroke to the idea of purely negative nature of Art. 8 ECHR right to privacy and absence of affirmative state obligations under the Convention in general.[342]

Two cases of this, third, type – *I.* v. *Finland*[343] and *K.U.* v. *Finland*,[344] are analysed further.

With regard to the facts of the *I.* v. *Finland* case, they are the following. The applicant, a Finnish national, worked as a nurse in a public hospital. During the period of her employment she was regularly consulting the same hospital's polyclinic for infectious diseases as she had been diagnosed as HIV-positive.

The case concerned the applicant's allegation that, following certain remarks made at work, she suspected that her colleagues had unlawfully consulted her confidential patient records kept in a hospital database and that the district health authority had failed to provide adequate safeguards against unauthorised access to her private medical records.[345] In support of her claim the applicant relied, among others, on Article 8 ECHR.

---

[338] ibid., p. 14.

[339] ECHR 2 December 2008, *K.U.* v. *Finland*, Application no. 2872/02. Paras. 36-39.

[340] Purtova, 'Private law solutions in European data protection', p. 13.

[341] ibid., p. 10.

[342] ibid.

[343] ECHR 17 July 2008, *I* v. *Finland***,** Application no. 20511/03.

[344] ECHR 2 December 2008, *K.U.* v. *Finland*, Application no. 2872/02.

[345] HUDOC Press Release.

The Government contended that there was no violation within the meaning of Article 8 as at the time there was national legislation in place[346] which "guaranteed the secrecy of a person's health information and, in principle, all patient information was kept secret. Only those participating in the patient's treatment were entitled to process data concerning him or her."[347]

The Court disagreed and held unanimously that there had been a violation of Article 8 on account of the domestic authorities' failure to protect, at the relevant time, the applicant's patient records against unauthorised access.[348]

"It is plain that had the hospital provided a greater control over access to health records … the applicant would have been placed in a less disadvantaged position before the domestic courts", the Court said.

The Court said that the mere existence of the right to claim compensation for damages caused by an alleged unlawful disclosure is not the same as protecting privacy in the first place.[349] "What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access".[350] Since such protection was not given, the Court couldn't but "conclude that at the relevant time the State failed in its positive obligation under Article 8 (1) of the Convention to ensure respect for the applicant's private life".[351]

In other words, although in time of the violation there was a national law in place making unauthorized access to medical files unlawful, and the violation of that law in fact led to violation of Article 8, the mere existence of general data protection rules is insufficient to fulfill the positive State duty. The State is also obliged to create an effective system of data security, making sure that other (also private) actors do not violate privacy protected by Article 8 ECHR.[352]

Thereby, first, *I.* v. *Finland* judgment may be interpreted to call if not for more detailed State regulation of data processing, surely for its better enforcement.[353] The case is particularly interesting as there was no statement in it proving that there was deliberate and unauthorized access to data, only that there was a failure on the part of the State to secure the data

---

[346] Purtova, 'Private law solutions in European data protection', p. 11.

[347] *I.* v. *Finland,* Paras. 31, 34.

[348] HUDOC Press Release.

[349] 'Data blunders can breach human rights, rules ECHR', in *OUT-LAW News*, 22 July 2008, viewed on 9 May 2011, <http://www.out-law.com/page-9287>.

[350] *I.* v. *Finland,* Para. 47.

[351] Out-Law.com, 'Data blunders can breach human rights, rules ECHR', in *OUT-LAW News.*

[352] Purtova, 'Private law solutions in European data protection', p. 12.

[353] ibid.

appropriately.[354]

But a key finding of the case was that the Court stated that personal information relating to a patient undoubtedly belongs to his or her private life.[355] This judgment confirmed a wide scope of the protected privacy rights and prepared a ground to include the entire body of data protection rules into privacy interests protected by Art. 8 ECHR.[356]

Another notable judgment, particularly significant for the current research as it tackles upon the issue of protection of personal data on the online social networking site, is the judgment in the case of *K.U.* v. *Finland.* This case is another illustration of the ECHR influence on the content of the State positive obligations under Article 8, hence also on the content of the data protection rules and private parties' obligations.[357]

In the case of *K.U.* v. *Finland* an unknown person had posted an advertisement of a sexual nature on an Internet dating site in the name of a 12 year old boy. Under Finnish law in place at that time, the police and the courts could not require the service provider (bound by the confidentiality of telecommunications) to reveal the identity of the person who had posted the ad. Any prosecution was therefore excluded. Ruling on the case, the ECtHR found that there had been a violation of Article 8 of the Convention stemming from the failure of the Finnish authorities to abide by the positive obligations to protect a child from invasion of his private life as enshrined in Article 8.[358]

In the *K.U.* v. *Finland*, the ECtHR seems to have made explicit use of the possibility opened in *I.* v. *Finland.* Namely, not only did it reaffirmed the existence and clarified the content of the state positive obligations under Article 8. It also gave guidelines the parties to the Convention as to the content of their data protection obligations regarding anonymity on the Internet.[359]

A cumulative reading of the aforementioned cases in general and of the decisions in *K.U.* v. *Finland* and *I.* v. *Finland* in particular leaves no doubt that the right to privacy as protected by Article 8 ECHR also implies positive State obligations, and therefore incorporates data protection interests.[360]

---

[354] Wordpress.com, 'ECHR: Surveillance Ruling (2008)', in *Where is Your Data?* 16 February 2009, viewed on 9 May 2011, <http://whereismydata.wordpress.com/tag/echr/>.

[355] ibid.

[356] Purtova, 'Private law solutions in European data protection', p. 12.

[357] Purtova, 'Private law solutions in European data protection', p. 12.

[358] HUDOC Press Release.

[359] Purtova, 'Private law solutions in European data protection', p. 12.

[360] ibid., p. 11.

Thus, summarizing the findings of the Court in the three lines of the case-law analysed above, they may be interpreted (in the data protection context) as calling for creation by the states-signatories of a comprehensive data protection systems which adhere to the ECHR principles and, as a result, indirectly bind private parties with the ECHR rules.[361]

Applying the theory of positive obligations to the Internet privacy, particularly to the information privacy in the sphere of social networking, would therefore entail proving that:
(i) privacy infringements committed by a certain SNS are so substantial that they amount to fundamental right's breach, and
(ii) the State ought to have regulated this field in order to prevent privacy infringements.[362]

This scheme fits perfectly in the picture of SNSs violating the right to privacy in data protection of the European users,[363] as such violations are made possible exactly by the reasons of failure on the part of the States to effectively channel (by means of legislation and law enforcement measures) the private parties' behaviour, in doing so stopping privacy-abusing practices.

It seems that, so far, as we considered the three lines of the ECHR cases, only one but important problem remains unsolved. It concerns the question of jurisdiction and originates from the fact that the current research deals with a cross-border Internet activities. Those companies, whose privacy-infridging practicies had been analysed before, have their officies outside of the European borders, namely – in the USA. Therefore, the application of the norms of the ECHR to this (American) private parties would mean, as some may argue, an inappropriate extention of the Court's jurisdiction beyond the borders of the Council of Europe States. Nevertheless, this possible argumentation is to be overcome in the last part of the current analysis by showning that the application of the ECHR rules in the context of a cross-border social networking is not only possible, but necessary as far as privacy violations concern the rights of the European citizens.

6.4 The fourth line of cases

Due to the global character of the modern online social networking and the absence of as regards the infrastructure frontiers, the processing operated by companies located outside of the national borders of the Council of Europe States might (and, as have been already demonstrated, in fact does) directly

[361] ibid., p. 12.

[362] Nawrot, Syska & Świtalski, p. 17.

[363] See Chapter 5.

affect the privacy of those residing on the such States' territories.[364]

Meanwhile the State parties to the ECHR have an obligation to secure the rights of their citizens within their *jurisdiction* (ECHR, Article 1). Jurisdiction is in ECHR case law understood as primarily territorial – "physically placed and described"[365] – other bases of jurisdiction being exceptional and requiring special justification.[366] However, the global nature of social networks with the absence of physical frontiers, challenges this territorial definition of jurisdiction, especially in cases of the protection of privacy, when activities conducted in one jurisdiction have effects in multiple jurisdictions, and thus can create a level of uncertainty as to a State's obligations.[367]

Nevertheless, the transborder character of the online networking doesn't by any means defeat the principle of territorial jurisdiction. Rather, the principle adapts itself to the specific situation of the Internet.[368]

What is meant by this is that the Internet (in the case we want our human rights to be protected) should be viewed not as some "out-of-law space", but rather as an extension of our existing public spaces.[369]

As have been pointed out by Mrs. Hanne Sophie Greve, a former judge at the ECtHR, "the fact that the Internet transcends national jurisdictions and is worldwide in nature holds the implication that it has an impact on every jurisdiction, it does not remove the Internet from the multiplicity of national jurisdictions. The Internet is neither beyond the law nor above the law – or the rule of law. In this respect, the Internet in its very essence is no different from other means of content delivery. From a rule of law perspective the main distinctive aspect of the Internet is its transjurisdictional character".[370]

Mrs. Hanne Sophie Greve continues to state further, that "it is never justified or acceptable to erode the rule of law or to undermine human rights

---

[364] Y Poullet, in *Council of Europe BLOGGED Submission to the Internet Governance Forum*, p. 22.

[365] J Kulesza, *Internet governance and the jurisdiction of States justification of the need for an international regulation of cyberspace*, 2008, p. 1, cited in G Hasselbalch, 'Privacy and Jurisdiction in the Global Network Society', May 2010, p. 2, <http://mediamocracy.files.wordpress.com/2010/05/privacy-and-jurisdiction-in-the-network-society.pdf>.

[366] ECHR 8 July 2004, *Ilascu and others* v. *Moldova and Russia*, Application no. 48787/99. Paras. 313-319, cited in Hasselbalch, p. 2.

[367] Hasselbalch, p. 2.

[368] R Uerpmann-Wittzack, 'Principles of International Internet Law', *German Law Journal*, vol. 11, No. 11, 2010, p. 1258, <http://germanlawjournal.com/pdfs/Vol11-No11/PDF_Vol_11_No_11_1245-1263_Articles_Uerpmann.pdf>.

[369] *Council of Europe BLOGGED Submission to the Internet Governance Forum*, p. 27.

[370] H S Greve, in *Council of Europe BLOGGED Submission to the Internet Governance Forum*, p. 11.

by delegation. The advent and existence of the Internet forms no exception in this respect and there is no reason why it should. It is furthermore, expected that every State is able to control and oblige every actor on its territory and within is jurisdiction. The case law of the ECtHR makes stringent demands on States in this respect."[371]

To sum up, it doesn't matter from where the violator comes. What is decisive is that the violations occur on the territory of the Member State to the Convention. This is definitely the case with the processing of personal data of the European users by the American companies, such as Facebook.

To the extent that private sector actors are relied upon to deliver services due by the State, they become agents of the latter. In full respect for Council of Europe standards and principles, including the freedom of communication on the Internet and the importance for States to encourage self-regulation and co-regulation regarding content disseminated on the Internet, this delegation brings with it a right and duty of oversight for the State concerned.[372] This duty imposes on the States parties to the ECHR positive obligations with regard to the protection of personal data of those individuals residing on their respective territories.

The idea can be understood also from the still sparse case law of the ECtHR as it addresses new aspects of the established human rights provisions raised by the Internet.[373]

In this regard the case of *Perrin* v. *the UK*[374] is of a crucial importance. It demonstrates that the ECHR case law gives no indication that the Strasbourg Court consider the Internet as a regime unto itself and/or beyond the realm of human rights.[375] Accordingly, it illustrates the transjurisdictional implications of online activities.[376]

The applicant, a French national residing in the UK, was a majority shareholder of a US company, which had created a website with obscene pornographic images. The site was operated and controlled in the US.[377]

However, the applicant was sentenced to 30 months in prison under the UK

---

[371] H S Greve, in *Council of Europe BLOGGED Submission to the Internet Governance Forum*, p. 26.

[372] *Council of Europe BLOGGED Submission to the Internet Governance Forum*, p. 8.

[373] H S Greve, in *Council of Europe BLOGGED Submission to the Internet Governance Forum*, p. 11.

[374] ECHR 18 October 2005, *Perrin* v. *UK* (Admissibility Decision), Application no. 5446/03.

[375] H S Greve, in *Council of Europe BLOGGED Submission to the Internet Governance Forum*, p. 11.

[376] Hasselbalch, p. 3.

[377] ibid.

Obscenity Act 1959 for making the material available online to minors in the UK.

In the application to the ECtHR, the applicant, relying on Article 10 ECHR, maintained that because of the worldwide nature of the Internet it was unreasonable for publishers to foresee the legal requirements in all individual States where the material could be accessed.[378] The applicant contended, inter alia, that his site complied with domestic United States legislation.[379]

Nevertheless, the Court found the complaint manifestly ill-founded, basing the reasoning on the following considerations.

The Court held that although the images in question might be legal in other States including non-State parties to the Convention, the government had not exceeded its margin of appreciation when prosecuting and convicting the applicant within its own territory.[380]

The Court considered that the existence of other protective measures (such as parental control software packages, making the accessing of the sites illegal and requiring Internet Service Providers (ISPs) to block access) had not rendered it disproportionate for the authorities to resort to criminal prosecution, particularly when those other measures have not been shown to be more effective.[381]

The Court added that the web page at issue was freely available to anyone surfing the Internet and that it included the very type of material which might be sought out by young persons whom the national authorities were trying to protect.[382]

The Court also observed that it would have been possible for the applicant to avoid the harm and, consequently, the conviction, while still carrying on his business, by ensuring that none of the photographs were available on the free preview page.[383]

The ECtHR considered the *effects* of the material and thus regarded the criminal conviction necessary in a democratic society[384] as the conviction

---

[378] ibid.

[379] *Council of Europe BLOGGED Submission to the Internet Governance Forum*, p. 15.

[380] Hasselbalch, p. 3; *Council of Europe BLOGGED Submission to the Internet Governance Forum*, p. 15.

[381] *Council of Europe BLOGGED Submission to the Internet Governance Forum*, p. 15.

[382] ibid.

[383] ibid.

[384] Hasselbalch, p. 3.

pursued the legitimate aim of protecting morals and rights of others.[385]

The decision seems quite reasonable in the light of a recognised principle of territorial jurisdiction in international law. Thus, e.g., this principle is reflected in Article 22 of the European Convention on Cybercrime (ECC) of 23 November 2001, confirming the traditional principle of territorial jurisdiction. According to Article 22(1)(a) ECC each contracting party establishes jurisdiction over offences committed on its territory. It is well established that an offence is committed at the place where the perpetrator acted.[386] If a person places harmful content, such as pornography on a web site, the State where the person has actually worked on the computer seems not to be of a decisive importance. Traditionally, it is accepted that an offence is committed on the territory where the effects of a criminal act occur.[387]

Therefore, as the Perrin case demonstrates, the case law of the ECtHR is now beginning to shape the positive obligations of the States with regard to the way rights and freedoms are exercised and protected online. So far, the ECtHR has underlined the right for Member States to take action to stop harmful Internet content from reaching children and young people.[388]

Other cases regarding the human right in data protection online will without any doubt emerge soon.[389] The author is positive with this regard, taking into account the dynamic nature of the Convention case law, demonstrated through the course of the analysis of the four lines of cases above.

One more testimony of this may be derived from the observed nature of the European privacy legislation, namely, its tendency to change in order to reflect the demands of the digital age, and, specifically, bearing in mind the expected data protection legislative review (in 2011).

Besides, though the ECHR case law dealing with cross-border Internet activities is limited, the Perrin case may provide an interpretative framework for the Strasbourg Court[390] and be indicative for the further direction, which the Court has to follow in order to ensure the further protection of the right to privacy.

As a living instrument, the Convention has no chances to remain indifferent to the changing privacy landscape.

---

[385] *Council of Europe BLOGGED Submission to the Internet Governance Forum*, p. 15.

[386] Oxman (note 51), para. 16, cited in Uerpmann-Wittzack, p. 1254.

[387] Uerpmann-Wittzack, p. 1254.

[388] *Council of Europe BLOGGED Submission to the Internet Governance Forum*, pp. 14-15.

[389] ibid., p. 15.

[390] Hasselbalch, p. 4.

Remindful of the fact that the Court is still at the early stage of dealing with the Internet transborder issues, the following fact has to be presented at the end of the current analysis.

In June 2009, Facebook in their response to a letter from the Danish Data Protection Authority, rejected the Article 29 group's interpretation of online jurisdiction[391] by emphasizing the physical placement of their equipment in the USA.[392]

Keeping in mind the ECtHR decision in Perrin case (together with all the previous decisions of the Court, which has shaped the concept of indirect horizontal effect of the Convention and started including data protection into the scope of the Article 8 right to privacy), the author hopes that the current paper's analysis has demonstrated the way in which the question about the effectiveness of measures taken by the Danish State to, e.g., secure the protection of Danish users on the SNSs, will be possibly assessed by the ECtHR in future.[393]

[391] See Opinion 1/2008 on data protection issues related to search engines, p. 11 under "Establishment on the territory of a member state (EEA)" - use of cookies requires adherence to the national law in question. Opinion 5/2009 on online social networking under "Who is the data controller?" cited in Hasselbalch, p. 4.

[392] Hasselbalch, p. 4.

[393] ibid.

Conclusion

The current research aimed to find out how the European legal system may approach the challenges of the online social networking and their effects on the right to privacy in personal data protection of the European users. Since the answer closely depends on the nature of the right in question (human right or property right), the instant research turned to a comparative analysis of the American and European privacy models. Having ruled on the human rights nature of personal data protection in Europe, as well as on the correspondent privacy abusing practices of the online social networking business, the examination concentrated on the Article 8 ECHR possibilities to protect the right. The analysis of the ECHR case law led to conclude on the matter of existence of positive obligations of the States parties to the Convention to ensure an effective enjoyment of the right to privacy of the European users of the SNSs, in a sense of a recognition of an indirect horizontal effect of the Convention's provisions on the relationships between the users of the services, from one hand, and the social networking companies, providing their services in Europe, - on the other (irrespective of the territories of the countries from which such services are provided – be they within the European borders, or, as is the case with Facebook and other the most popular social networking platforms, - within the borders of the USA).

At the European level, the Council of Europe's Member States are under a positive obligation to act in a proactive manner with a view to securing the effective enjoyment of protected rights, for example by taking reasonable measures designed to protect those under their jurisdiction from certain forms of harm in the context of Internet services. The failure to do so may render a State liable under the ECHR,[394] if it can be established that the State has failed to take appropriate measures within its power to protect the individuals under its jurisdiction[395] from the right to privacy violations on the part of, *inter alia*, American social networking companies.

Thus, when considering the emerging trends in online social networking and in anticipation of potential (as well as of already existing) human rights violations in connection with its use, Council of Europe Member States need to prepare themselves to deal with situations related to Article 8[396] with regard to the practices of treating the other people's personal data by online business.

Without any doubt, much remains to be done and there are still many unanswered questions regarding the interpretation of the right to privacy in

---

[394] *Council of Europe BLOGGED Submission to the Internet Governance Forum,* p. 12.

[395] ibid., p. 17.

[396] ibid., p. 16.

online situations[397] which, as the author sincerely hopes, the current research has helped to analyse and map out, pointing at the future directions on the path of balancing the ever-increasing digital technologies with the needs to ensure that individuals' human rights are not sacrificed at the expense of the modern developments.

Nevertheless, as we are still at the beginning of this process and the Court has just started developing its case law with regards to the regulation of online environment, one of the tools an individual anyway has to protect his or her privacy is to think before sharing their personal data.

[397] ibid., p. 24.

Bibliography

Articles, Books and Web Documents

- Acquisti, A, 'Awareness, Understanding, and Individual Decision-Making', *OECD Conference.* Heinz College/CyLab, Carnegie Mellon University, October 26, 2010, <http://www.oecd.org/dataoecd/33/40/46943626.pdf>.
- Akandji-Kombe, J-F, *Positive obligations under the European Convention on Human Rights. A guide to the implementation of the European Convention on Human Rights*, Human rights handbooks, No. 7, Council of Europe, 2007.
- Bail, FLe, 'Discours d'ouverture', *Speech on the Data Protection Day*, Brussels, 28 January 2011, <http://www.data-protection-day.net/files/Introduction_0_3_Francoise_Le_Bail_speech_FINAL_OK_FOR_WEBSITE.pdf>.
- Barrigar, J, J Burkell & I Kerr, 'Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information'. *Canadian Business Law Journal*, vol. 44, <http://www.idtrail.org/files/LETS_NOT_GET_PSYCHED_OUT_OF_PRIVACY%20final%5B1%5D.pdf>.
- Barrigar, J, 'Social Network Site Privacy: A Comparative Analysis of Six Sites', in *Office of the Privacy Commissioner of Canada*, February 2009, <http://www.priv.gc.ca/information/pub/sub_comp_200901_e.cfm>.
- Beddard, R, *Human Rights and Europe*, Cambridge University Press, 1994.
- Benn, SI, *Privacy, Freedom, and Respect for Persons*, in R J Pennock & J W Chapman (Eds.), Privacy. New York: Atherton Press, 1971.
- Bergkamp, L, 'EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy', *Computer Law & Security Report*, vol. 18, No. 1, 31 January 2002, <http://www.hunton.com/files/tbl_s47Details/FileUpload265/499/Privacy_fallacy.pdf>.
- Bernier, C, 'Online Behavioral Advertising and Canada's Investigation on Facebook. Remarks at the Privacy Laws and Business 23rd Annual Conference', in *Office of the Privacy Commissioner of Canada*. Cambridge, United Kingdom, July 6, 2010, <http://www.priv.gc.ca/speech/2010/sp-d_20100706_cb_e.cfm>.

- Bernier, C, 'Personal Data Protection Issues in a Globalized World. Remarks at the 3rd Conference of Francophonie Personal Data Protection and Privacy Commissioners', in *Office of the Privacy Commissioner of Canada*. Madrid, Spain, November 3, 2009, <http://www.priv.gc.ca/speech/2009/sp-d_20091103_cb_e.cfm>.
- Blok, P, *Het recht op privacy (The right to privacy)*, The Hague: Boom Juridische Uitgevers, 2002.
- Bonneau J, & S Preibusch, 'The Privacy Jungle: On the Market for Data Protection in Social Networks'. *The Eighth Workshop on the Economics of Information Security*, WEIS, 2009, <http://preibusch.de/publications/Bonneau_Preibusch__Privacy_Jungle__2009-05-26.pdf>.
- Busch, A, 'From Safe Harbour to the Rough Sea? Privacy Disputes across the Atlantic', *SCRIPT-ed*, vol. 3, issue 4, June 2006, <http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/busch.asp>.
- Bygrave, LA, 'Privacy and Data Protection in an International Perspective'. *Stockholm Institute for Scandinavian Law*, 2010, <http://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Privacy%20and%20Data%20Protection%20in%20International%20Perspective.pdf>.
- Cavoukian, A, 'When Online Gets Out of Line. Privacy: Make an Informed Online Choice', in Information and Privacy Commissioner, Ontario, 2006, <http://www.ipc.on.ca/images/Resources/up-facebook_ipc.pdf>.
- Clapham, A, *Human Rights in the Private Sphere*, Clarendon Press Oxford, 1993, <http://classes.lls.edu/fall2006/intlhumanrgts-romano/documents/HumanrightsClapham.pdf>.
- *Council of Europe BLOGGED Submission to the Internet Governance Forum*, Athens, Greece, 30 October to 2 November 2006, <http://www.coe.int>.
- Clarke, R, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms', in *Roger Clarke's Web-Site*, 15 August 1997, viewed on 7 May 2011, <http://www.rogerclarke.com/DV/Intro.html>.
- Cuijpers, C, 'A Private Law Approach to Privacy; Mandatory Law Obliged?', *SCRIPTed*, vol. 4, issue 4, September 2007.
- Denham, E, 'PIPEDA Case Summary #2009-008: Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act', in *Office of the Privacy Commissioner of Canada*. 2009, <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm>.

- Docksey, C, ‘EU Data Protection: The Development of a New Right of Privacy in Europe’, Warsaw, 10 March, 2007, <http://www.cels.law.cam.ac.uk/events/Docksey_30March.pdf>.
- EPIC.org, ‘Social Networking Privacy’, in *Electronic Privacy Information Center*, viewed on 9 May 2011, <http://epic.org/privacy/socialnet/#back>.
- European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*, Publications Office of the European Union, Luxembourg, 2010, <http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf>.
- Evans, DS, ‘The Online Advertising Industry: Economics, Evolution, and Privacy’, University College London and University of Chicago, April 2009, <http://www.intertic.org/Policy%20Papers/EvansEOAI.pdf>.
- Foutouchos, M, ‘The European Workplace: The Right to Privacy and Data Protection’. *Accounting Business & the Public Interest*, vol. 4, No. 1, 2005, <http://visar.csustan.edu/aaba/Foutouchos.pdf>.
- Friedewald, M, ‘A New Concept for Privacy in the Light of Emerging Sciences and Technologies’. *From the SelectedWorks of Michael Friedewald*, April 2010, <http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=michael_friedewald>.
- Gellman, R, ‘Fair information practices: A Basic History’, Version 1.82, April 19, 2011, <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>.
- Gray, MTD, J Hester & J E Cole, *Uniform Standards to Protect the Privacy of Personal Information: A Study of the International Trend to Protect Privacy in Personal Information*, Office of Information Practices, January 2000, <http://www.state.hi.us/oip/reports/privrptappb.pdf>.
- Harris, DJ, M O’Boyle & C Warbrick, *Law of the European Convention on Human Rights*, Oxford University Press, New York, 2009.
- Hasselbalch, G, ‘Privacy and Jurisdiction in the Global Network Society’, May 2010, <http://mediamocracy.files.wordpress.com/2010/05/privacy-and-jurisdiction-in-the-network-society.pdf>.
- Hert, PDe, & S Gutwirth, ‘Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence in the Institute for Prospective technological studies’, *Security and Privacy for the citizen in the post-September 11 digital age: a Prospective overview*,

2003.

- Hugenholtz, B, 'The Commodification of Information: The Future of the Public Domain', *Institute for Information Law,* Amsterdam, January 2004, <http://www.ivir.nl/agenda/iter/PapersCommodification/Final%20Background%20Paper1.doc>.
- Humanrightsfirst.org, 'Business And Human Rights', in *Human Rights First*, viewed on 5 May 2011, <http://www.humanrightsfirst.org/our-work/business-and-human-rights/>.
- Illmer, A, 'Data protection commissioner warns over social networking sites', in *DW-WORLD.DE Deutsche Welle*, 27 December 2009, viewed on 9 May 2011, <http://www.dw-world.de/dw/article/0,,5060457,00.html>.
- International Working Group on Data Protection in Telecommunications, *Report and Guidance on Privacy in Social Network Services. "Rome Memorandum"*, 43rd meeting, 3-4 March 2008, Rome (Italy).
- Jagland, T, Secretary General of the Council of Europe, *Speech made on the Data Protection Day (30th Anniversary)*, Brussels, 28 January 2011, <http://www.data-protection-day.net/files/Introduction_0_1_SG_Jagland_OK_FOR_WEBSITE_FINAL.pdf>.
- Jones, H, & JH Soltren, *Facebook: Threats to Privacy*, 14 December 2005, <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf>.
- Kacimi, K, S Ortolani & B Crispo, 'Anonymous Opinion Exchange over Untrusted Social Networks'. *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*, Nuremberg, Germany, March 31, 2009, <http://www.inf.unibz.it/~mkacimi/eurosys2009.pdf>.
- Kohnstamm, J, 'New European Rules on Data Protection?' Speech at *Joint High Level Meeting on Data Protection Day*, 28 January 2010, <http://www.data-protection-day.net/files/Panel_1_4_Jacob_Kohnstamm_Speech_OK_for_website.pdf>.
- Laurant, C, *Privacy & Human Rights 2003: An International Survey of Privacy Laws and Developments*, Electronic Privacy Information Center, Washington, DC, USA, Privacy International, London, UK, 2003, <https://www.privacyinternational.org/survey/phr2003/index.htm>.
- Lundblad, N, 'Privacy in a Noise Society'. St Anna Institute, Stockholm, 2004, <http://www.sics.se/privacy/wholes2004/papers/lundblad.pdf>.

- Martin, K, 'Facebook (A): Beacon and Privacy', *Business Roundtable Institute for Corporate Ethics*, The Catholic University of America, 2010, <http://www.darden.virginia.edu/corporate-ethics/pdf/Facebook%20_A_business_ethics-case_bri-1006a.pdf>.
- Michael, J, *Privacy and Human Rights: An International and Comparative Study, With Special References to Developments in Information Technology*, Dartmouth: UNESCO Pub., Aldershot: Paris, 1994.
- Michael, J, *Privacy*, in D Harris & S Joseph, *The International Covenant on Civil and Political Rights and United Kingdom Law*, London, Clarendon Press, 1995.
- Miller, AR, *Assault on Privacy: Computers, Data Banks and Dossiers*, Michigan, MichiganUP, 1971.
- Mitrano, T, 'Facebook 2.0'. *EDUCAUSE Review*, vol. 43, no. 2, March/April 2008, <http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume43/Facebook20/162687>.
- Nawrot, F, K Syska & P Świtalski, 'Horizontal application of fundamental rights: Right to Privacy on the Internet', *9th Annual European Constitutionalism Seminar*, University of Warsaw, May 2010, <http://en.zpc.wpia.uw.edu.pl/wp-content/uploads/2010/04/9_Horizontal_Application_of_Fundamental_Rights.pdf>.
- Office of the Information and Data Protection Commissioner, 'Online Behavioural Advertising', <http://idpc.gov.mt/dbfile.aspx/Behavioural_advertising.pdf>.
- Organisation for Economic Co-operation and Development, *The Evolving Role of the Individual in Privacy Protection: 30 Years after the OECD Privacy Guidelines*, 32 International Conference of Data Protection and Privacy Commissioners, Jerusalem, Israel, 27-28 October 2010, <http://www.oecd.org/document/44/0,3746,en_2649_34255_45780844_1_1_1_1,00.html>.
- Out-Law.com, 'Data blunders can breach human rights, rules ECHR', in *OUT-LAW News*, 22 July 2008, viewed on 9 May 2011, <http://www.out-law.com/page-9287>.
- Prins, C, 'Property and Privacy: European Perspectives and the Commodification of our Identity'. *The future of the public domain*. Tilburg University, The Netherlands, 2006.
- Privacy International, 'Social Network Sites and Virtual Communities', in *Privacy International*, 18 December 2007, viewed on 9 May 2011, <https://www.privacyinternational.org/article/phr2006-privacy-topics-social-network-sites-and-virtual-communities>.

- Purtova, N, ‘Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights’. *Netherlands Quarterly of Human Rights*, vol. 28, No 2, 2010, <http://arno.uvt.nl/show.cgi?fid=106377>.
- Purtova, N, ‘Property in Personal Data: a European Perspective on the Instrumentalist Theory of Propertisation’. *European Journal of Legal Studies*, 2010, 2, 3, The Future of... Law & Technology in the Information Society, <http://cadmus.eui.eu/bitstream/handle/1814/15124/10_Property_EN.pdf?sequence=1>.
- Råman, J, ‘European Court of Human Rights: Failure to take effective information security measures to protect sensitive personal data violates right to privacy – I v. Finland, no. 20511/03, 17 July 2008’, *Computer Law & Security Report 24*, 2008.
- Reding, V, ‘Why the EU needs new personal data protection rules’, Speech 10/700 at the *European Data Protection and Privacy Conference*, Brussels, 30 November 2010, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700&format=HTML&aged=0&language=EN&guiLanguage=en>.
- Reidenberg, JR, & PM Schwartz, ‘Data Protection Law and On-line Services: Regulatory Responses’, *European Commission's Office of Official Publications*, Luxembourg, 1998, <http://ec.europa.eu/justice/policies/privacy/docs/studies/regul_en.pdf>.
- Roberson, M-R, ‘Online Social Networks: Finding a Balance Between Sharing and Privacy’, in *DukeToday*, 12 November 2010, viewed on 9 May 2011, <http://today.duke.edu/2010/11/cox.html>.
- Roggensack, M, ‘Facebook Confuses “Security” and “Privacy”’, in *Human Rights First*, 28 January 2011, viewed on 9 May 2011, <http://www.humanrightsfirst.org/2011/01/28/facebook-confuses-“security”-and-“privacy”/>.
- Roggensack, M, ‘Face It Facebook, You Just Don’t Get It’, in *Human Rights First*. May 25, 2010, viewed on 5 May 2011, <http://www.huffingtonpost.com/human-rights-first/face-it-facebook-you-just_b_589045.html>.
- Rosen, J, ‘The Web Means the End of Forgetting’, *The New York Times*, 21 July 2010, <http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html>.
- Sassen, S, *The Topoi of E-Space: Private and Public Cyberspace*, viewed on 6 May 2011, <http://fortunaty.net/com/textz/textz/sassen_saskia_the_topoi_of_e-space.txt>.

- Schneier, B, 'Facebook and Data Control'. *A blog covering security and security technology,* September 21, 2006, viewed on 6 May 2011, <http://www.schneier.com/blog/archives/2006/09/facebook_and_da.html>.
- Shiels, M, 'Twitter co-founder Jack Dorsey rejoins company', in *BBC News. Business*. 28 March 2011, viewed on 5 May 2011, <http://www.bbc.co.uk/news/business-12889048>.
- Slemmons Stratford, J, & J Stratford, 'Data Protection and Privacy in the United States and Europe', *IASSIST Conference*, Yale University, New Haven, Connecticut, May 21,1998, <http://www.iassistdata.org/downloads/iqvol223stratford.pdf>.
- Solove, DJ, M Rotenberg & P M Schwartz, *Privacy, information, and technology*, Aspen Publishers, 2006.
- Solove, DJ, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy'. *Stanford Law Review*, 2001, No 53.
- Stoddart, J, 'Privacy in the era of social networking: Legal obligations of social media sites. Remarks at the University of Saskatchewan College of Law Lecture Series', in *Office of the Privacy Commissioner of Canada*. Saskatoon, Saskatchewan, November 22, 2010, <http://www.priv.gc.ca/speech/2010/sp-d_20101122_e.cfm>.
- Stoddart, J, 'The Path to Proactive Privacy. Remarks at the 1st Annual Privacy and Information Security Congress 2010 organized by Reboot Communications Ltd.', in *Office of the Privacy Commissioner of Canada*. Ottawa, Ontario, November 15, 2010, <http://www.priv.gc.ca/speech/2010/sp-d_20101115_e.cfm>.
- Stoddart, J, 'Why Privacy Still Matters in the Age of Google and Facebook and How Cooperation Can Get Us There. Remarks at the 2010 Access and Privacy Conference', in *Office of the Privacy Commissioner of Canada*. Edmonton, Alberta, June 10, 2010, <http://www.priv.gc.ca/speech/2010/sp-d_20100610_e.cfm>.
- Sullivan, B, ''La difference' is stark in EU, U.S. privacy laws', in Privacy Lost on msnbc.com, 19 October 2006, viewed on 8 May 2011, <http://www.msnbc.msn.com/id/15221111/ns/technology_and_science-privacy_lost/>.
- Swire, P, 'Social Networks, Privacy, and Freedom of Association. How Individual Rights Can Both Encourage and Reduce Uses of Personal Information'. *Center for American Progress*, February 2011, <http://ftc.gov/os/comments/privacyreportframework/00342-57843.pdf>.
- Tavenerslaw.co.uk, 'Are social networks and European data privacy

laws incompatible?' in *Taveners*. May 2010, viewed on 6 May 2011, <http://www.tavenerslaw.co.uk/social-networks>.

- Terwangne, C, 'Is a Global Data Protection Regulatory Model Possible?', in *Reinventing Data Protection?*, S Gutwirth, Y Poullet, P De Hert, C de Terwangne & S Nouwt (eds), Springer, 2009.
- Uerpmann-Wittzack, R, 'Principles of International Internet Law', *German Law Journal*, vol. 11, No. 11, 2010, <http://germanlawjournal.com/pdfs/Vol11-No11/PDF_Vol_11_No_11_1245-1263_Articles_Uerpmann.pdf>.
- Vegheş, C, C Pantea, D Bălan & B Lalu, 'European Union Consumers' Views on the Protection of their Personal Data: an Exploratory Assessment'. *Annales Universitatis Apulensis Series Oeconomica*, 11(2), 2009, <http://oeconomica.uab.ro/upload/lucrari/1120092/44.pdf>.
- Westin, A, *Privacy and Freedom*, London, Bodley Head, 1967.
- Wordpress.com, 'ECHR: Surveillance Ruling (2008)', in *Where is Your Data?* 16 February 2009, viewed on 9 May 2011, <http://whereismydata.wordpress.com/tag/echr/>.
- Zwick D, & N Dholakia, 'Models of Privacy in the Digital Age: Implications for Marketing and E-Commerce'. *American University, University of Rhode Island*, September 7, 1999, <http://ritim.cba.uri.edu/Working%20Papers/Privacy-Models-Paper%5B1%5D.pdf>.

Hard and Soft Law

- Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, adopted on 22 June 2010, 00909/10/EN, WP 171, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf>.
- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 (Convention 108).
- Directive 2002/58/EC of 12th July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (ePrivacy Directive).
- Directive 97/66/EC of 15th December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.
- Directive 95/46/EC of 24th October 1995 on the Protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive).
- Directive 2006/24/EC of 15th 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 (Data Retention Directive 2006/24/EC6).

- EU Charter of Fundamental Rights 2000.
- European Commission, *A comprehensive approach on personal data protection in the European Union*, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee of the Regions, Brussels, 4 November, 2010, COM(2010) 609 final, <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf>.
- European Convention on Cybercrime (ECC) 2001.
- European Convention on Human Rights 1950.
- *Explanations relating to the Charter of Fundamental Rights*, prepared under the authority of the Praesidium of the Convention which drafted the Charter of Fundamental Rights of the European Union, 2007/C 303/02, <http://eur-lex.europa.eu/en/treaties/dat/32007X1214/htm/C2007303EN.01001701.htm>.
- Lisbon Treaty 2007.
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980.
- Regulation (EC) 45/2001/EC4 of 18th 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 (Data Protection Regulation).

Table of Cases

- ECHR 23 July 1968 *'Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium'* v. *Belgium*, Applications no. 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64.
- ECHR 21 April 1979, *Marckx* v. *Belgium*, Application no. 6833/74.
- ECHR 9 October 1979, *Airey* v. *Ireland,* Application no. 6289/73.
- ECHR 26 March 1985, *X. and Y. v. The Netherlands*, Application no. 8978/80.
- ECHR 7 July 1989, *Gaskin* v. *UK*, Application no. 10454/83.
- ECHR 16 December 1992, *Niemitz* v. *Germany*, Application no. 13710/88.
- ECHR 24 June 2004, *Von Hannover* v. *Germany*, Application no. 59320/00.
- ECHR 8 July 2004, *Ilascu and others* v. *Moldova and Russia*, Application no. 48787/99.
- ECHR 18 October 2005, *Perrin* v. *UK* (Admissibility Decision), Application no. 5446/03.
- ECHR 17 July 2008, *I v. Finland***,** Application no. 20511/03.
- ECHR 2 December 2008, *K.U.* v. *Finland*, Application no. 2872/02.
- ECHR 15 April 2009, *Reklos and Davourlis* v. *Greece*, Application no. 1234/05.