HORIZONTAL APPLICATION OF FUNDAMENTAL RIGHTS: RIGHT TO PRIVACY ON THE INTERNET

François Nawrot
Katarzyna Syska
Przemysław Świtalski

9th Annual European Constitutionalism Seminar
University of Warsaw
May 2010

CONTENTS

Introduction

"In the digital world consumers are subject to far more intrusive data gathering by businesses and government than in the past. Moreover, as their personal information is collected, large organizations have become increasingly secretive. Personal information is also more often used for data-mining, behavioral targeting for marketing purposes, compiling personal name records and credit scoring. There is a risk that these developments undermine basic human rights of individuals to autonomy and control of their personal information."[1]

This essay looks into the threats posed by the widespread Information and Communication Technologies (ICTs) usage to their users' privacy. The analysis involves the question whether the legislation currently in force affords sufficient protection to users' privacy. Furthermore, the issue of applying fundamental rights horizontally is addressed, i.e. whether, given the necessity to ensure ICTs users' appropriate protection, the fundamental right to privacy may be invoked against private parties.

The right to privacy, just like any other fundamental right, was traditionally guaranteed as a protection against the abuses of power by public authorities. However, private entities often have the possibility to exert considerable influence on people's lives, including the spheres protected by basic rights. This is certainly the case of ICTs, where private parties play a major role in their development and control. Hence, the risk of privacy infringements may result not only from public authorities' actions, but also those of private parties. For that reason, there is a recent tendency to oblige private parties to be bound by certain provisions regarding the fundamental rights protection. For instance, in the context of privacy protection, private parties already have the duty to protect users' personal data on the same level as public authorities are obliged to do so.

This paper will first give a brief characterization of the right to privacy and a few examples of court opinions regarding privacy protection. Then, the threats to users' privacy in the digital world, not just those regarding personal data processing, will be presented. Further, the current legal framework of personal data and consumer protection will be analyzed to see if these regulations can be relied upon in cases regarding Internet to users' privacy. Finally, the essay will focus on the possibility to invoke the fundamental right to privacy against private entities and on the theory of positive obligations of the state to assure appropriate protection of fundamental rights.

[1] Trans Atlantic Consumer Dialogue: *Charter of Consumer Rights in the Digital World*. Doc No. INFOSOC 37-08. March 2008. P 4.
http://tacd.org/index.php?option=com_docman&task=cat_view&gid=83&Itemid=40 [retrieved: Apr 25, 2010].

General Remarks on Right to Privacy

The right to privacy is certainly one of the most important within the EU legal framework. It is guaranteed by Art. 8 of the European Convention of Human Rights as well as by Art. 7 of the Charter of Fundamental Rights of the European Union (CFR), not the mention national constitutions.

Both documents contain a very general statement that everyone has the right to respect for their private and family life, home and communications. A detailed definition is lacking - "[p]rivacy is not a static object that can be defined, it is always context related, making it impossible to define it without referring to a complex net of social, cultural, religious, and historical parameters from which it delivers its meaning."[2] Thus, providing a precise definition of privacy would be both impossible and inoperative – the very aim of such abstract concept is to adapt to the changing social and political circumstances. Nevertheless, a brief description of what could fall within the category of privacy protection shall be presented.

In its resolution on mass communication media and human rights, the Parliamentary Assembly of the Council of Europe stated the following: "The right to privacy consists essentially in the right to live one's own life with a minimum of interference. It concerns private, family and home life, physical and moral integrity, honor and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorized publication of private photographs, protection against misuse of private communications, protection from disclosure of information given or received by the individual confidentially."[3]

The European Court of Human Rights found an infringement on privacy on various occasions: violation of secrecy of correspondence (i.e. monitoring one's correspondence), even in case of detainees and prisoners[4]; interception of telephone conversations[5]; a search of a person's home without a warrant and without impartial observers[6]. The Court noted that such violations of privacy are not always absolutely forbidden, but the legislation regulating limitations of privacy should be precise, foreseeable and proportionate, i.e. privacy restriction must not exceed what is justified by the legitimate aim pursued[7].

The European Court of Human Rights also declared that a person's right to protection of his or her reputation is encompassed by the right to respect for private life[8]. Another occasion

---

[2] Schermer, Bart Willem: *Software Agents, Surveillance, and the Right to Privacy*. Leiden University Press. 2007. P 71.

[3] Parliamentary Assembly of the Council of Europe: *Resolution No 428 (1970) containing a declaration on mass communication media and human rights.* Part C. Art. 2. Text adopted by the Assembly on 23 January 1970 (18th Sitting).
http://assembly.coe.int//Main.asp?link=http://assembly.coe.int/Documents/AdoptedText/TA70/ERES428.htm [retrieved: Apr 25, 2010].

[4] e.g. ECHR cases *Vitan v. Romania* (No. 42084/02), *Cavallo v. Italy* (No. 9786/03), *Moiseyev v. Russia* (No. 62936/00).

[5] e.g. ECHR case *Kruslin v. France* (No. 11801/85).

[6] e.g. ECHR case *Varga v. Romania* (No 73957/01).

[7] Renucci, Jean-François: *Introduction to the European Convention on Human Rights : the rights guaranteed and the protection mechanism*. Strasbourg. Council of Europe Publications 2005. P 46.

[8] e.g. ECHR case *Pfeifer v. Austria* (No. 12556/03)

which the Court deemed to be a privacy violation was a refusal of access to one's file (concerning their identity and personal information)[9].

With the proliferation of ICT usage, the right to privacy is getting more attention. The reason behind it is that Information Technology offers unprecedented possibilities of surveillance of Internet users[10]. That, in turn, may result in ubiquitous privacy infringements.

The development of ICTs gave rise to a new concept regarding the right to privacy, i.e. *informational privacy* or *informational self-determination*[11]. This notion implies that everyone shall have the right to decide what information about them is communicated, and in what way. This idea is reflected in one of the resolutions of the Council of Europe's Parliamentary Assembly, which proposes to extend the definition of privacy previously given – "the right to live one's life with a minimum of interference"[12]. "In view of the new communication technologies which make it possible to store and use personal data, the right to control one's own data should be added to this definition."[13]

As it was already noted, privacy breaches on the Internet may occur not only as acts of public authorities, but also, and perhaps prevalently, of private entities. The paper shall now look at the types of data concerning Internet users collected by private actors and how such data is further processed.

[9] e.g. ECHR case *Gaskin v. United Kingdom* (No. 10454/83).
[10] *Civil Society Background Paper. Fueling Creativity, Ensuring Consumer and Privacy Protection, Building Confidence and Benefiting from Convergence.* Recommendations and Contributions to the OECD Ministerial Meeting of 17-18 June 2008 from Civil Society Participants in the Public Voice Coalition. Pp 21-22. http://thepublicvoice.org/events/seoul08/cs-paper.pdf [retrieved: Apr 25, 2010].
[11] Schermer, Bart Willem: *Software Agents, Surveillance, and the Right to Privacy*. Leiden University Press. 2007. P 87.
[12] Parliamentary Assembly of the Council of Europe: *Resolution No 428 (1970)* … See: footnote 3.
[13] Parliamentary Assembly of the Council of Europe: *Resolution No 1165 (1998). Right to privacy*. Art. 5. Text adopted by the Assembly on 26 June 1998 (24th Sitting). http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta98/ERES1165.htm [retrieved: Apr 25, 2010].

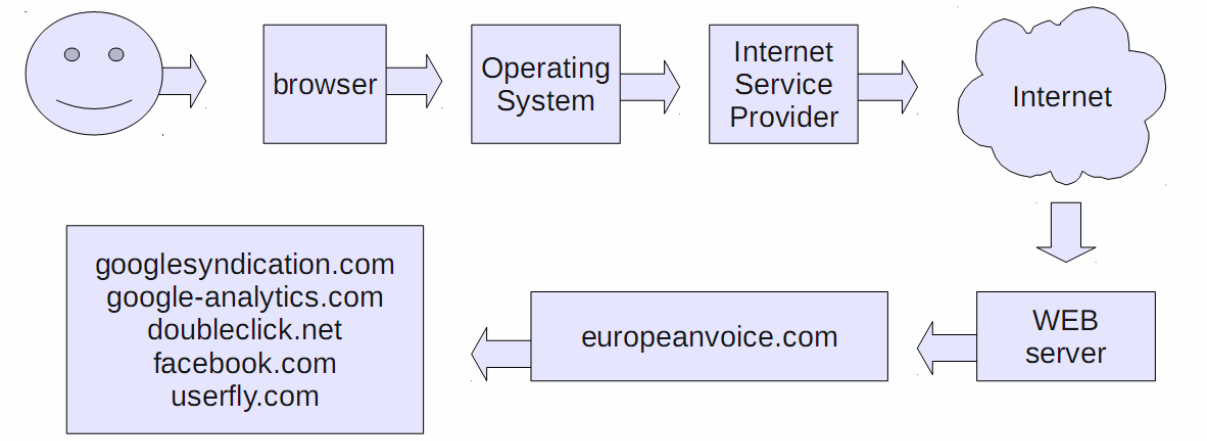
How Privacy Is Threatened Online

"Remember that every transaction you make, every site you visit on the Internet, leaves traces. These "electronic tracks" can be used, without your knowledge, to build a profile of what sort of person you are and your interest."[14]

Information society „forces" people to spend more and more time on-line everyday. People use the Internet to communicate with others, to do business, to seek information, to buy goods and services. People browse the web looking for information, send e-mails, use instant messengers, download movies, shop, etc. At all times, Internet users and their behavior online might be observed by various service providers. In this chapter, however, we shall focus on web browsing and how user's privacy can be violated by electronic services providers.

In the examples presented in this paper we concentrate on services offered by Google, Inc. and Facebook, Inc., because of their popularity and amount of information concerning them available. The reader should, however, bear in mind that practices such as those described below are commonplace and used by most electronic services providers.

When looking at typical session of Internet user viewing web page it seems fairly simple from the outside – a user inputs a web address, and then they can browse the desired page. If one looks at what is happening from a more technical perspective, the picture is much more complicated. The scheme presented below demonstrates how many parties may be involved in a simple act of web-browsing.



Simplified[15] scheme of act of web-browsing

Let us look at the example of the "European Voice" website. A user's web-browser requests a server to send a website. The server sends the website's code, and the browser shows the desired website. But since the website contains pieces of code from third parties, these parties are also "informed" about a particular user's "presence" on the European Voice website. This

[14] Committee of Ministers of the Council of Europe: *Recommendation No R (99) 5. Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways*. Adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers' Deputies. Part II. Art. 2.

[15] The main simplification is the box representing third parties, all of which in reality interact directly with user's web browser, possibly involving other third parties.

may be done by the way of installing the so-called "cookie" files on user's browser. Cookies usually "tag" browsers with unique identifying numbers, which in turn allows them to recognize returning users and collect information on their on-line behavior. Such information collection might not be cookie-based, but his is the most common practice. In the case of http://europeanvoice.com/[16] viewers, the third parties involved include: DoubleClick, Facebook, Userfly and Google, at least two of which (Userfly and Google) are placed in website's source code only to watch users' on-line behavior. Each of these entities can store information on users (especially their browsing history) and create user profiles. What is more, if users are at the same time logged on to any Google service account[17] (e.g. Gmail, Picassa), the profile built during their web browsing may by connected to their account. (Examples of cookies placed on users' computers by a few popular websites are shown in Appendix 1.)

The same algorithm works for Facebook, the only difference being that even unknowledgeable users can in most cases easily check whether Facebook is included on web page (by a visible Facebook frame[18] with the "Like" button or "join the fan page" option). If a user is logged on to Facebook[19] while browsing websites containing Facebook frames, then Facebook might connect their web browsing history to their Facebook profile even if the user does not click on the Facebook frame on a webpage visited.

This type of user behavior-logging happens on nearly every page. It might be performed in a way that is impossible for users to notice on any server when the analysis concerns only users' behavior inside one server[20]. What a well-informed user might notice is that most web servers use third-party tools which enable them to track their users. Such tools, on one hand, make it easier for web developers to create and monitor their services and, on the other, allow certain Internet companies (like Google, Facebook, Gemius) to keep track of users' activities.

Other possible means of privacy infringement may actually concern secrecy of correspondence. Not all users are aware of Google (and other e-mail providers') practice – automated e-mail content analysis. According to Google, only computer software is involved in "reading" e-mails (thus no human interference is necessary). The mail is analyzed in order to find out what the users' interests may be so that the most suitable and appealing advertisements are addressed to a particular user on the side of the window. It is precisely for that reason that ads visible in Google's e-mail service are usually connected to contents of an e-mail message which is read at a given moment.

Privacy threats in the digital world are countless; the examples named above are just a few most frequent ones[21]. It should be therefore noted that Internet users are hardly ever explicitly

[16] Source code of the website retrieved on May 1, 2010.
[17] Google will also be able to recognize people that logged on to any of their Google accounts during last 2 years and have not deleted their cookies since then.
[18] Please note, however, that on some occasions a simple "Like" will not result in Facebook being informed about the user's presence on a given website. Facebook will only receive such information if displaying the webpage involves generating data from Facebook servers (e.g. pictures of people that currently „like" a page).
[19] Facebook similarly to Google is able to recognize their user if such user has logged in on Facebook during the past 2 years and did not delete cookies since.
[20] Such analysis and further results storage might be done based on dynamic web pages generation, which is not visible for internet users.
[21] To find out more about other possible privacy threats, see e.g.: *Cloud Computing. Benefits, risks and recommendations for information society*. A report of the European Network and Information Security Agence. November 2009; King, Nancy J.: *When Mobile Phone Are RFID-Equipped – Finding E.U.-U.S. Solutions to*

informed that their online activity is observed by quite a few different entities. Relevant information can be sometimes found in a website's terms and conditions or privacy policy, but it is not always the case. Furthermore, even if a "cookie notice" is introduced in a website's terms, it is hardly ever clear and comprehensive. Perhaps users should be informed about data that is collected on them and about their profiling for the purposes of behavioral targeting. And so the question may be raised whether positive steps should be taken to ensure that Internet users are given clear and comprehensible notice about threats to their privacy (e.g. whenever data about them is collected). Another question to be answered is naming the party (parties) responsible for raising users' awareness, e.g. online services providers, Internet service providers, web browser producers, etc.

Taking into account the possible privacy infringements described above, new measures aimed at raising users' awareness of privacy risks are desirable, especially bearing in mind what certain Internet "decider" recently said. Eric Schmidt (CEO of Google) stated: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place"[22]. From the point of view of the fundamental right to privacy, such reasoning is certainly flawed.

Protect Consumer Privacy and Facilitate Mobile Commerce. Michigan Telecommunications and Technology Law Review. 2008. Vol. 15. P 107.

[22] [in:] Larkin, Eric: *Will Cloud Computing Kill Privacy?* PC World. March 2010. P 44.

Privacy Protection under Current Legal Framework

The right to privacy has been recognized from the beginning of our civilization. First of all Christianity, Judaism and Islam took it into account in their respective writings. In the Qur'an some verses directly deal with privacy such as:

> "Do not spy on one another"[23] or "Do not enter any houses except your own homes unless you are sure of their occupants' consent"[24].

With the development of the modern State all over Europe the right to privacy was increasingly considered to be a protection against the State itself and its possible infringements. We better understand this while reading William Pitt who, as a member of parliament, wrote in 1763:

> "The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter – but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement".

More and more the right to privacy tended to be recognized by national laws, especially in the nineteenth century. For instance, the French civil code (better known as the Napoleon code), which came into force in 1804, provided:

> "Everyone is entitled to the respect of his private life"[25] .

The first international recognition of the right to privacy came with the Universal Declaration of Human Rights of 1948:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."[26]

A few years later the European Convention for the Protection of Human Rights signed in Rome in 1950 adopted a similar rule:

> "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."[27]

---

[23] Qur'an (49:12)
[24] *Ibid*. (26:42)
[25] French Code civil, Art. 9.
[26] Universal Declaration of Human Rights of 1948. Art. 12.
[27] European Convention of Human Rights of 1950. Art. 8.

In 1966 the International Covenant on Civil and Political Rights adopted by the General Assembly of the United Nations provided:

> "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[28]

It is therefore clear that the right to privacy is recognized worldwide. We shall now turn to the problems of privacy online and analyze how it can be protected under the legislation currently in force.

Personal Data Protection

At the end of the 1960's the right to privacy was recognized by various international and regional treaties and/or conventions. However, new technologies developed and the treatment of personal data with computers led to new challenges. The notion of the right to privacy seemed to be too wide to efficiently deal with these new issues. In the 1970's some European countries adopted new statutes particularly connected with privacy and informatics. The Land of Hessen in Germany was the first in Europe to adopt such a statute in 1970. Sweden and France respectively in 1973 and 1978 came later but were still among the first European countries to deal with such new issues.

From this time „data protection" has been increasingly used to define the sub-part of privacy dealing especially with informatics. However, privacy and data protection were still considered as a protection against the State. Here the French example is particularly relevant. In the early 1970's the French government wanted to create a new informational system. This project relied on the idea of identifying each citizen with a unique number giving access to all his/her data coming from different administrations (social security, ministry of home affairs, etc.). It came to an end and later on another government decided to adopt a new statute dealing with informatics, files and freedoms. This statute was designed to provide the citizens with certain rights against the State such as the right to access data, or the right to modify incorrect data. A national committee responsible for informatics and freedoms was also created[29].

In 1980 the Organization for Economic Co-operation and Development (OECD) issued a general guidance note on the Protection of Privacy and Transborder Flows of Personal Data[30]which indicated a few core principles to protect privacy and personal data. One should mention that these guidelines are not binding since they are considered soft-law. A year later the Council of Europe issued the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as the Convention no. 108[31]. The convention explains that its purpose is "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental

[28] International Covenant on Civil and Political Rights of 1966. Art. 17(1).
[29] Commission National de l'Informatique et des Libertés (CNIL)
[30] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris 1980.
[31] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg 1981.

freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").”[32]

Until now it has been the only international convention dealing specifically with data protection. When it was adopted by the Council of Europe Internet did not exist (at least not in its present shape) so the Convention did not take it into account.

As far as European Union is concerned, the first text of importance related to data protection was the European Directive 95/46/EC[33]. As the directive points it out, the main goal ascribed to Member States is to “protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.”[34]

The Directive defines “personal data” as “any information relating to an identified or identifiable natural person (“data subject”'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”[35].

This definition is wide enough and seems to include a lot of different situations. It is “any” information connected with an “identified” as well as “identifiable” natural person. This person can be identified “directly” as well as “indirectly” with different factors connected with various aspects of his/her identity. The definition provided by the directive seems to encompass many possibilities. E-mail addresses and IP (Internet Protocol) addresses are sometimes regarded as personal data. Moreover, search engines such as Google retain search queries of users. A single search query usually does not give information about one's identity, but compiling hundreds or thousands of them amounts to a real user profiling and is likely to give quite a precise idea of one's identity. The question then arises whether users' profiles (created for the purposes of behavioral targeting) could be regarded as personal data. Are they tantamount to the notion of „any information” contained in the directive? It seems that if such a profile is linked to one's account on a given website, then the information about that user's search history might also be considered personal data.

Quite a few important principles regarding personal data processing are contained in this directive. Different provisions give an efficient framework to data processing. Certain conditions have to be met in order to carry on data processing, e.g. the data subject has unambiguously given his consent to data processing[36] and the data subject has to be informed by the data controller about their right to access, modify and erase personal data concerning them.[37].

The Directive 95/46/EC also created a Working Party on the Protection of Individuals with regard to the Processing of Personal Data[38] also known as G29. This institution gathers all the Member States’ authorities responsible for data protection and takes common positions.

---

[32] *Ibid*. Art. 1.
[33] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[34] *Ibid*. Art. 1.
[35] *Ibid*. Art. 2(a).
[36] *Ibid*. Art. 7(a).
[37] *Ibid*. Art. 10.
[38] *Ibid*. Art. 29.

Another European Directive concerning personal data was adopted in 1997, namely the Directive 97/66/EC[39]. One should also mention the Charter of Fundamental Rights of the European Union. Though proclaimed in 2000, the Charter came into force only on December 2009, together with the Treaty of Lisbon. In the Charter, there is a distinction between privacy and protection of personal data Art. 8 of the Charter reads as follows:

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

Even if such a shift appeared already in late 1970's and in early 1980's, the Internet probably played a significant role in distinguishing between privacy and data protection. When the Charter was drafted in late 1990's, its drafters probably had in mind what twenty or thirty years before nobody would have considered possible (in what regards the development of new technologies and especially the Internet, and the revolution stemming from it as far as personal data are treated).

The directive 2002/58/EC[40], also known as e-privacy directive was adopted to face the treats to privacy posed the Internet. This directive has been modified in 2009 so as to take into account new developments, but also to eliminate some of the original shortcomings.

In Art. 5, the e-privacy Directive guarantees the confidentiality of communications. Surveillance and of communications and related traffic data is prohibited, unless with a user's consent or unless it is legally authorized. Art. 5(3) regulates storing of and access to information stored in user's terminal equipment (e.g. cookie files stored by user's browser). Such storing is only permissible when the "user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing". It may therefore be concluded that cookie use is conditional on user's informed consent. Whether a vague "cookie notice" in a website's terms and conditions is enough to count as "clear and comprehensive information" is certainly debatable.

The evolution of personal data protection could be seen from different angles. On one hand, personal data protection arose with the development of informatics in the 1970's and in the 1980's. It developed first on national levels before being recognized by international conventions such as the Convention no. 108 of the Council of Europe, but also by the European law in numerous directives and an explicit recognition in the Charter of Fundamental Rights. However, one cannot assert that personal data protection is no more connected with the general right to privacy. It is a sub-part of it which has its own rules and specificities, but still personal data protection is a part of the right to privacy. On the other hand, personal data protection has undergone a significant evolution within the last thirty years. Coming from a general right to privacy it first aimed at protecting citizens against violations committed by the State. Personal data protection now seems increasingly to be a

[39] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.
[40] Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

safeguard provided for citizens not only against the State and its infringements on privacy, but also, and maybe foremost, against private entities, recently especially providers of services on the Internet. Personal data protection thus advanced from a vertical relationship between the State and its citizens towards a theoretical horizontal one between private parties. We will see later why such a horizontal relationship is not necessarily horizontal or at least equal.

Consumer Protection

Some scholars[41] have compared the current situation for the Internet and its regulation with the development of consumer protection. The main idea on which this analogy relies is to follow the same way in regulating the Internet as the one which governed when lawyers started regulating mass consumption. One of the main similarities is probably the situation of mass consumption at the beginning of the 20th century and that of the Internet today. As Benjamin R. Sachs points out „Today, the new jungle is not an economy of industry but one of information, a place where telecommunications have changed the way services reach today's consumers in much the same way that the railroad changed the way goods reached consumers of the 1900s"[42]. Faced with new situations do we necessarily need new solutions? According to Sachs, consumer protection can apply to the new issues rising on the Internet. Indeed users of the Internet, while surfing, are often consumers whereas service providers seem to be real entrepreneurs. With the beginning of mass consumption we faced the development of big companies which were unable, but also unwilling to bargain with each consumer while selling a good or a service. Therefore there was an inequality in the process of bargaining between consumers and entrepreneurs. Adhesion contracts are probably a significant symbol of such a relationship. Susan E. Gindin argued that privacy policies on the Internet bear the comparison with adhesion contracts[43]. Indeed privacy policies are often required to be read before accessing a website. They contain some details about the way personal data of the user/consumer are going to be used. However, these privacy policies are rarely read by users/consumers. Susan E. Gindin quotes a recent survey of the University of California in her article explaining why privacy policies are ineffective. It would be because of the following reasons:

(1) Privacy policies are too difficult to read;
(2) [P]rivacy policies lead consumers to believe that their privacy is protected.

Even if they could understand them, the amount of time required to read privacy policies is too great. A 2008 study estimated that if users actually read privacy policies, it would take approximately 200 hours a year to read the policy for every unique website visited in a year, not to mention updated policies for sites visited on a repeating basis[44]. This kind of behavior has been called „click-happiness" when users just want to use a new website or download a new program. According to Susan E. Gindin, this is foremost due to a "lack of awareness"[45].

[41] e.g. Benjamin R. Sachs, Susan E. Gindin (see below).
[42] Sachs, Benjamin R.: *Consumerism and Information Privacy: How Upton Sinclair Can Again Save Us From Ourselves*. Virginia Law Review 2009. Vol. 95. P 207.
[43] Gindin, Susan E.: *Nobody reads you Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*. Northwestern Journal of Technology and Intellectual Property 2009. Vol. 8. No 1. P 14.
[44] *Ibid*. P 21. Susan E. Gindin quotes the following reference: UNIV. OF CAL. BERKELEY, SCHOOL OF INFORMATION, KNOWPRIVACY 11 (June 1, 2009) (emphasis in original), *available at* http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.
[45] *Ibid*. P 36.

Should we agree with Benjamin R. Sachs's opinion:"No matter how careful users are, it seems that only internet abstinence can guarantee consumers' privacy"?[46]

According to Susan E. Gindin this is not specifically connected with the Internet since she observed that „[c]onsumers have signed contracts without reading them for decades"[47]. However, the question is not to know whether a user reads privacy policy before agreeing to the general terms of use. The question is whether a user/consumer had the possibility to read it before agreeing. Usually, if a privacy policy was available prior to the agreement, it does not matter to know whether the user read it. It is binding like a normal contract if all information was available. However, some cases showed that service providers/entrepreneurs made their privacy policies available only after the subscription of the user/consumer. Applying basic rules of consumer protection to the Internet could also solve questionable issues as far as contracts are concerned. This is already what happens in the United States especially thanks to the Federal Trade Commission (FTC). It has to deal with consumer protection and has been increasingly faced with Internet-related problems and the right to the privacy seen from a contractual angle. The FTC can apply to privacy policies rules coming from the consumer protection such as for example: "Where the other party has reason to believe that the party manifesting such assent would not do so if he knew that the writing contained a particular term, the term is not part of the agreement"[48]. One could imagine the same reasoning for a privacy policy. A particularly unfavorable term could probably deter the user/consumer from agreeing to such a contract if they knew about it.

Such issues arose with some tracking applications which tracked users for commercial and advertising purposes. These applications are able to profile users' needs or desires by analyzing their researches on search engines. It leads to the distinction between the "opt-out" and"opt-in" clauses in website's terms. There is an "opt-out" clause when a user is able to withdraw their consent to a particular privacy setting. But in the case of an "opt-out" there is a default setting which usually is not favorable to the user's privacy. They can modify it but they are often not informed about the possibility to opt out. On the contrary, an "opt-in" clause describes a situation where a setting connected with the user's privacy needs their direct and positive agreement. As far as privacy and personal data protection are concerned, the model based on "opt-in" clauses would be more compliant with consumer protection that the model based on the "opt-outs".

Another interesting comparison between mass consumption and the Internet is the concept of product labeling. From the beginning of the 20th century, food law regulated the labeling of products according to specific rules connected with quality, geographical origin and traditions. There are also some short notices like nutrition labels, providing consumers with understandable information. As Susan E. Gindin noted it in her article, a few scholars are advocating the idea of such "labels" for websites in order to give to consumers a basic idea about which data would be collected about them and for what purpose[49]. Actually, as the survey conducted by the Berkeley University showed privacy policies are often too long to be read by users, a short notice on top of a page could provide users with a general idea of the website's privacy policy.

[46] Sachs: *Consumerism and Information Privacy* … P 231.
[47] Gindin: *Nobody reads* … P 22.
[48] *Ibid*. P 15.
[49] *Ibid*. P 27.

Faced with these new challenges, some companies or institutions adopt self-regulatory principles for the Internet as far as privacy and personal data protection are concerned. Benjamin R. Sachs advocates something totally new as far concerning data protection: a „general tort liability for breach of information privacy"[50], still bearing in mind the lessons of consumer protection. The newest idea of this general tort would have a very wide scope of application. Benjamin R. Sachs thus explains:"The scope of the tort, therefore, should cover any entity, whether corporate or individual, that provides goods or services and in the process digitally stores personal and identifying information"[51]. Such a general tort would probably deeply modify the current notion of information privacy and contribute to a horizontal application of personal data protection.

[50] Sachs: *Consumerism and Information Privacy* … P 239-250.
[51] *Ibid*. P 240.

Positive Obligations of the State

Should the protection of private information by personal data and consumer legislation prove insufficient, do the users have any other recourse…? Quoting the fundamental right to privacy seems plausible, though it should be remembered that its applicability to relations between private parties is problematic.

European Convention on Human Rights Framework

The idea of negative obligations of the state is inherent in the European Convention of Human Rights and it basically implies that a state should refrain from certain actions, or, in other words, should not interfere in the exercise of fundamental rights[52]. Positive obligations, on the other hand, entail a duty of a state to "intervene" – i.e. to provide appropriate legislation to "secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention" (Art. 1 of the European Convention). That idea was first brought up in the *Belgian linguistic case*[53], but it was stated in a more straightforward manner in the *Airey* case: "The Convention is intended to guarantee not rights that are theoretical or illusory but rights that are practical and effective."[54]

The Court also ruled that states shall "ensure that the right of persons under their jurisdiction to their image is respected by third parties, including journalists."[55] This case (*von Hannover v. Germany*[56]) actually concerned the Princess Caroline of Monaco. The pictures containing details of her private life were published in German press. The Court said that the German state ought to clarify its legislation regarding the privacy of public figures. This judgment is particularly interesting as it imposes upon a state a duty to regulate relations between private parties (here: the extent to which privacy of public figures may be intruded by journalists).

Another notable case, and particularly important to this study as it concerns privacy on the Internet, is the *K.U. v. Finland*[57] judgment. The facts of the case are the following: someone put an ad of a twelve-year old boy on an Internet dating site. The ad contained the boy's picture, age, a detailed description of his physical characteristics and an information that the boy was looking for an intimate relationship with a boy of his age or older. The boy was thus exposed to receiving unwanted messages, also from pedophiles. The boy's father asked the police to identify the person who put the ad online so that he could bring charges against that person. But the Internet service provider refused to reveal that information, citing its duty to ensure confidentiality of telecommunications. Subsequently the national courts found that there was no relevant provision in Finnish legislation which would allow for disclosure of that person's identity.

[52] Akandji-Kombe, Jean-François: *Positive Obligations under the European Convention on Human Rights*. Human rights handbook no. 7. Council of Europe. Strasbourg 2007. P 5.
[53] ECHR case *"Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium" v. Belgium* (No 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64).
[54] ECHR case *Airey v. Ireland* (No. 6289/73).
[55] Akandji-Kombe: *Positive Obligations…* P 39.
[56] ECHR case *von Hannover v. Germany* (No. 59320/00).
[57] ECHR case *K.U. v. Finland* (No. 2872/02).

The Court decided that in this case, sufficient protection of one's privacy was not provided, because the applicant had no legal means to pursue the wrong that was committed against him and no possibility of redress. The Court reiterated that "although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life" (para 42). The Court goes on to say that "[t]hese obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves." (para 43). Thus, the Court recognizes the idea that the Convention may be indirectly held to regulate relations between private parties.

The decision also states that the exact nature of state's obligation to ensure respect for private life depends on the circumstances of the case. But with respect to this particular situation, the Court concluded that "practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case such protection was not afforded." (para 49).

The theory of positive obligations of the state is the notion that allows for horizontal application of the European Convention of Human Rights. It shall be nevertheless noted that within the ECHR framework, fundamental rights regulate relations between private parties only indirectly. Obviously, one cannot bring an action against a private entity before the Strasbourg Court. Neither can any infringement of a provision of the Convention by a private party result in ruling against a state. That private entity's infringing act has to be regarded as originating from the state's failure to sufficiently protect given basic right[58], i.e. it would not have occurred if appropriate legislation was in force.

It should also be noted that a decision finding a state's failure to regulate a given field bears more significant consequences than that finding a state's improper interference. The former imposes a duty to enact legislation that would meet the requirements of adequate fundamental rights protection (while the latter only requires that the state just repeal regulations that are at variance with the Convention)[59].

Applying the theory of positive obligations to Internet privacy would therefore entail proving that: (i) privacy infringements committed by certain ICT companies 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.

[58] Akandji-Kombe: *Positive Obligations…* P 14.
[59] Delmas-Marty, Mireille (ed.): *The European Convention for the Protection of Human Rights: international protection versus national restrictions.* Martinus Nijhoff Publisher. 1992. P 92.

Jurisprudence of the European Court of Justice

One of the most notable cases concerning horizontal application of fundamental rights and fundamental freedoms was the *Viking Line*[60] judgment. Viking Line was a Finnish shipping company that operated on the route between Helsinki and Tallinn. The company informed its workers that it intended to reflag its vessel under the Estonian flag so that it could enter into a new collective agreement with their workers based on Estonian labor law. The Finnish workers were members of a trade union affiliated with the International Transport Workers' Federation (ITF), which requested its affiliate in Estonia not to hold talks with Viking Line. Also, ITF announced its intention to strike if a new collective agreement (proposed by ITF under Finnish labor regulations) with Viking Line's employees was not concluded.

Viking Line decided to bring an action against ITF, raising the argument of infringement of its freedom of establishment. ITF, in turn, invoked the right to take collective action.

Thus, the Court had to decide whether the fundamental freedom of establishment could be relied upon by a private party in an action against another private party. The Court reaffirmed "that the fact that certain provisions of the Treaty are formally addressed to the Member States does not prevent rights from being conferred at the same time on any individual who has an interest in compliance with the obligations thus laid down" (para 58). Thus, the ECJ stated that provisions pertaining to fundamental freedoms are to be observed not only by Member States, but also by private actors. Consequently, the Court confirmed that (in exceptional situations) bringing a claim based on fundamental freedoms infringement against a private party is permissible under the Treaty.

The Court also underlined that fundamental rights form an integral of the general principles of Community law, but "the exercise of that right may none the less be subject to certain restrictions" (para 44).

Whether the logic of horizontal application of fundamental freedoms can be applied to fundamental rights is obviously a controversial question. As it was noted before, obligations resulting from fundamental rights are primarily addressed to state actors. It is the duty of a given state to ensure that its legislation is in conformity with basic rights and that sufficient protection is afforded to all persons within its jurisdiction. If such protection is lacking, the established way to obtain it leads through the theory of positive state obligations, i.e. an action against a state has to be commenced, alleging the state's failure to guarantee one's basic rights on a proper level. Needless to say – this is the long way.

In order to argue in favor of the horizontal application of fundamental rights, one should first of all bear in mind that the European Court of Justice emphasized the significance of fundamental rights protection within the EU legal order on numerous occasions. "Fundamental rights are one of the organising principles of the EU legal order. It can thus be argued that it is the commitment of this legal order to ensure that those rights are effectively protected regardless of whether the source of their violation is private or public conduct."[61]

---

[60] ECJ case C-438/05. *International Transport Workers' Federation and Finnish Seamen's Union* v *Viking Line ABP and OÜ Viking Line Eesti*.

[61] Krzeminska-Vamvaka, Joanna: *Horizontal effect of fundamental rights and freedoms – much ado about nothing? German, Polish and EU theiries compared after Viking Line*. Jean Monnet Working Paper 11/09. P 51. http://centers.law.nyu.edu/jeanmonnet/papers/09/091101.html [retrieved: Apr 26, 2010].

Another argument justifying the application of fundamental rights between private parties is that the classical approach to horizontal and vertical relations has been recently called in to question. Due account has to be taken of the tendencies such as globalization and privatization, and the fact that certain non-state actors (especially large multinational corporations) influence people's lives in a manner often comparable to that of states[62]. Therefore, a claim that such non-state actors should be subject to scrutiny akin to that to which states have to submit, is not entirely unfounded.

All in all, it seems that the possibility of ECJ authorizing the horizontal application of fundamental rights between private parties is not totally inconceivable.

[62] Länsineva, Pekka: *Fundamental Rights, Privatization and Private Power*. Paper presented during the 7th World Congress of the International Association of Constitutional Law (IACL). Athens, June 11-15, 2007. http://www.enelsyn.gr/papers/w10/Paper by Pekka Lansineva.pdf [retrieved: Apr 27, 2010].

Conclusions

There is hardly any doubt that one's privacy is exposed to a far greater threat in the Information Age than ever before. It also seems that users should be better informed about the privacy risks they may encounter when using the Internet. It is noteworthy such privacy infringements are often blamable on non-state actors.

The right to privacy online is partly guaranteed through personal data protection legislation. Throughout the years, we have seen an evolution of personal data regulations. In the beginning the goal was to protect individuals against abuse of power by state authorities. But as more and more private entities began collecting significant amounts of personal data, the duty to protect it was extended to those private parties. Of course in this case the horizontal effect of personal data protection was achieved indirectly as relevant legislation was first enacted that imposed certain obligations concerning personal data protection upon private entities.

The situation of Internet users can also be compared with that of consumers (especially that most Internet users would qualify as consumers). Even though consumers and entrepreneurs both belong to the group of private subjects, and so their situation should theoretically be equal, modern legal systems recognize the disparity in the consumer-entrepreneur relations. Obviously a consumer is the weaker party, and this disproportion is corrected by the consumer protection legislation. It seems that the weaker position of an Internet user should also be recognized.

The above-mentioned observations could also serve as arguments for a wider application of the fundamental right to privacy. The European Court of Human Rights allows it thanks to the theory of positive obligations of the state. The European Court of Justice recognized the direct horizontal applicability of fundamental freedoms. Taking into account the growing importance of certain non-state actors, the classical approach to fundamental rights might seem outdated. Especially that legal systems now affirm that even in relation between private parties, some of them are in a dominant position.

The question of horizontal application of fundamental rights is of course debatable. But one should bear in mind the rapid evolution of the modern world, and the tendencies of globalization or privatization. „Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society."[63] One might just as well imagine that besides new rights, such changes would bring about an updated model of their application.

[63] Warren, Samuel and Brandeis, Louis: *The Right to Privacy*. Harvard Law Review 1890. Vol. IV. No. 5.

Bibliography

Case-law

1. ECHR case *Vitan v. Romania* (No. 42084/02)
2. ECHR case *Cavallo v. Italy* (No. 9786/03)
3. ECHR case *Moiseyev v. Russia* (No. 62936/00)
4. ECHR case *Kruslin v. France* (No. 11801/85)
5. ECHR case *Varga v. Romania* (No 73957/01)
6. ECHR case *Pfeifer v. Austria* (No. 12556/03)
7. ECHR case *Gaskin v. United Kingdom* (No. 10454/83)
8. ECHR case *"Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium" v. Belgium* (No 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64)
9. ECHR case *Airey v. Ireland* (No. 6289/73)
10. ECHR case *von Hannover v. Germany* (No. 59320/00)
11. ECHR case *K.U. v. Finland* (No. 2872/02)
12. ECJ case C-438/05. *International Transport Workers' Federation and Finnish Seamen's Union* v *Viking Line ABP and OÜ Viking Line Eesti*

Legal acts

1. Committee of Ministers of the Council of Europe: *Recommendation No R (99) 5. Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways*. Adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers' Deputies
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg 1981Parliamentary Assembly of the Council of Europe: *Resolution No 428 (1970) containing a declaration on mass communication media and human rights*. Text adopted by the Assembly on 23 January 1970 (18th Sitting)
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
4. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector
5. Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
6. European Convention of Human Rights of 1950
7. International Covenant on Civil and Political Rights of 1966
8. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris 1980
9. Parliamentary Assembly of the Council of Europe: *Resolution No 1165 (1998). Right to privacy*. Text adopted by the Assembly on 26 June 1998 (24thSitting)
10. Universal Declaration of Human Rights of 1948

Books

1. Akandji-Kombe, Jean-François: *Positive Obligations under the European Convention on Human Rights*. Human rights handbook no. 7. Council of Europe. Strasbourg 2007
2. Delmas-Marty, Mireille (ed.): *The European Convention for the Protection of Human Rights: international protection versus national restrictions*. Martinus Nijhoff Publisher 1992
3. Renucci, Jean-François: *Introduction to the European Convention on Human Rights : the rights guaranteed and the protection mechanism*. Strasbourg. Council of Europe Publications 2005
4. Schermer, Bart Willem: *Software Agents, Surveillance, and the Right to Privacy*. Leiden University Press 2007

Articles

1. Gindin, Susan E.: *Nobody reads you Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*. Northwestern Journal of Technology and Intellectual Property 2009. Vol. 8. No 1
2. King, Nancy J.: *When Mobile Phone Are RFID-Equipped – Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce*. Michigan Telecommunications and Technology Law Review. 2008. Vol. 15. P 107
3. Krzeminska-Vamvaka, Joanna: *Horizontal effect of fundamental rights and freedoms – much ado about nothing? German, Polish and EU theories compared after Viking Line*. Jean Monnet Working Paper 11/09
4. Länsineva, Pekka: *Fundamental Rights, Privatization and Private Power*. Paper presented during the 7th World Congress of the International Association of Constitutional Law (IACL). Athens, June 11-15, 2007
5. Larkin, Eric: *Will Cloud Computing Kill Privacy?* PC World. March 2010. P 44
6. Sachs, Benjamin R.: *Consumerism and Information Privacy: How Upton Sinclair Can Again Save Us From Ourselves*. Virginia Law Review 2009. Vol. 95
7. Warren, Samuel and Brandeis, Louis: *The Right to Privacy*. Harvard Law Review 1890. Vol. IV. No. 5

Other

1. *Civil Society Background Paper. Fueling Creativity, Ensuring Consumer and Privacy Protection, Building Confidence and Benefiting from Convergence.* Recommendations and Contributions to the OECD Ministerial Meeting of 17-18 June 2008 from Civil Society Participants in the Public Voice Coalition
2. *Cloud Computing. Benefits, risks and recommendations for information society*. A report of the European Network and Information Security Agence. November 2009
3. Trans Atlantic Consumer Dialogue: *Charter of Consumer Rights in the Digital World*. Doc No. INFOSOC 37-08. March 2008

Appendix – Cookie files installed by different websites

Websites visited	Cookies acquired during a session
http://edition.cnn.com/ http://edition.cnn.com/2010/US/05/03/gulf.oil.spill.main/index.html?hpt=T2 http://edition.cnn.com/BUSINESS/	.cnn.com .doubleclick.net .facebook.com .scorecardresearch.com ads.cnn.com markets.money.cnn.com
http://www.economist.com/ http://www.economist.com/opinion/displaystory.cfm?story_id=16007299http://www.economist.com/opinion/	.addthis.com .atdmt.com .bluekai.com .collective-media.net .doubleclick.net .economist.com .fastclick.net .feedroom.com .fetchback.com .invitemedia.com .nexac.com .quantserve.com .revsci.net .roiservice.com .scorecardresearch.com .turn.com ad.yieldmanager.com www.economist.com

http://www.europeanvoice.com/ http://www.europeanvoice.com/article/2010/05/eurozone-leaders-to-hold-summit-friday-evening-/67855.aspx http://www.europeanvoice.com/page/policies-energy/1122.aspx	userfly.com .addthis.com .doubleclick.net .europeanvoice.com .facebook.com .imrworldwide.com
http://www.rp.pl/temat/2.html http://www.rp.pl/artykul/2,470388_Plama_ropy_zagraza_Ameryce.html http://www.rp.pl/temat/337506.html	cm2.atmitv.pl www.rp.pl rp.tabelaofert.pl .bs.serving-sys.com .facebook.com .go.arbopl.bbelements.com .hit.gemius.pl .nuggad.net .rzeczpospolita.pl .serving-sys.com
http://aw.gov.pl/ http://aw.gov.pl/pol/witamy.html http://aw.gov.pl/pol/kontakt.html	.hit.gemius.pl .stat.4u.pl
http://www.teatrwielki.pl/repertuar.html http://www.teatrwielki.pl/repertuar/opera.htm http://www.teatrwielki.pl/teatr_wielki/miejsce/historia.html	.teatrwielki.pl .youtube.com
http://wikipedia.org/ http://pl.wikipedia.org/wiki/Strona_g%C5%82%C3%B3wna http://pl.wikipedia.org/wiki/Lemoniada	--
http://www.zpc.wpia.uw.edu.pl/ http://en.zpc.wpia.uw.edu.pl/ http://www.zpc.wpia.uw.edu.pl/index.php	.zpc.wpia.uw.edu.pl .google.com