Law Aspects of Internet Information Privacy in the European Union

Daniel Eberharter

June 4, 2014

1 Introduction

It seems that nowadays the internet is everywhere - in every office, in every home, in every pocket. People are sharing their experiences, feelings, and interest on various social media pages, nobody needs to go outside to go shopping anymore and even job applications are done online.

All this results in massive amounts of valuable personal information, from which some companies make a fortune[1]. But can everyone access this information at will, or is there some kind of protection?

The following pages give a definition of information privacy and an explanation of the EU laws concerning it.

2 What is Information Privacy?

Information privacy is one of the fundamental human rights. The *European Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR) defines it as follows:

> [1]Article 8 Right to respect for private and family life
>
> - Everyone has the right to respect for his private and family life, his home and his correspondence.
> - There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, [...] or for the protection of the rights and freedoms of others.

Let us analyze the two sections of this definition separately.

[1]All hail the mighty Google

The first part defines the bounds of the right for privacy, with the controversial aspect being the right for respect of *correspondence*, which basically means that every citizen of a European Union country has a right for privacy regarding *all of his or her communication.*

The second half of the definition opens up a possibility for the public authority to restrict the right for privacy and states in which cases this limitation is appropriate.

In some cases it could be very hard to judge if and in what form such an act is necessary. The easiest way to identify a scenario, in which it is needed to limit the right for privacy, would be to compare the scenario to precedence cases [2].

3 Information Privacy on the Internet

Online communication differs from other forms of correspondence concerning information privacy. For example a new form of personal information appears - the behavioral data. Many websites store browsing history to recreate a schematic picture of the personality and the preferences of their visitors. Although this *tracking* may sound bad for the costumer it could have applications which create a better online experience for the user [3].

The real problem emerges when you add personal identifying information (name, address, day of birth, etc.) to behavioral data. From that data professionals can create a shockingly precise image of a person, without the subjects approval, like a class project of two students at the MIT (Massachusetts Institute of Technology) has shown [2]. Certer Jernigan and Behram Mistree developed an algorithm that took data from follow students' social-media accounts (not only their own personal data, but also the influence of befriended accounts) and predicted with 79 percent accuracy if that person is homosexual.

Although the practical application of such an algorithm are limited without a doubt, this a shocking example of how much personal information on the internet (given voluntarily or not) can be used to deduce further information.

The first laws regulating online data collection and preserving user privacy where introduced in the 1970s by the U.S. Department of Health, Education and Welfare. [4]

These laws influenced the European Directive on Data Protection which was introduced 1998 and contained rules to protect user privacy and regulated data collection.

[2] Since according to the German chancellor Angela Merkel the internet is "Neuland" these precedence cases might not be available.

[3] e.g.: the suggestion of products in online Stores.

4 The Data Protection Directive

The Data Protection Directive (Directive 95/46/EC) is a collection of articles which provide basic instructions on regulation and processing of the data of EU citizens and was adopted 1995.

Before this directive the treatment of personal information within the European union was handled only through guidelines of the *Organization for Economic Cooperation and Development* (OECD). [8]

The huge issue with the OECD principles was, that they were not binding. Information protection was still handled differently in each EU country and therefore information exchange between countries was very hard to achieve.

The Data Protection Directive is based on the following fundamental principles: [7]

- Limitation of data collection and procession
  - Transparency - When processing personal data the owner of the data has to agree[4] and the subject who processes the data has to identify itself (article 8).
  - Legal Purpose - The reason for data collection has to be explicit and legal (article 6b).
  - Limitation - The collected data quantities must not exceed the amount necessary to fulfill the purpose of the collection and may not be stored longer than needed (article 6).
- Transfer of Data to non-EU countries is only legit if the third party countries have a adequate level of protection (article 29).
- The government of each EU-country has to create a supervising authority which controls and regulates data collection following the laws of the Data Protection Directive.

5 The Data Retention Directive

The Data Retention Directive (or Directive 2006/24/EC) was one of the most discussed issues of privacy restriction in 2014. It forced each country in the European Union to record all electronic communication of their respective citizens for a minimum of six months (and a maximum of two years). The directive was made on 15 March 2006 and came into force only two months later on 3 May 2006[6]
Although collected data could only be accessed by the executive authorities through court permission, the idea of getting their data recorded led to a chorus of outrage within the European people, as well as several human rights groups and legal experts.

[4] exceptions: data access by the authority, necessity to fulfill a contract or the protection of the data owner

If we look at the first point of the ECHR definition of information privacy in section 2 we can obviously conclude that this directive contradicts with what the European Court of Human Rights defines as *Right to respect for private and family life*. The definition clearly states that *"Everyone has the right to respect for [...] his correspondence"*.

But here is where the second point of the definition creates an opening: *"There shall be no interference by a public authority [...] except such as is in accordance with the law and is necessary [...] in the interests of national security [...]"*

The obvious reason for keeping track of citizen communication is crime prevention. But crime cannot be prevented if there has to be a court order in the first place to view the recorded data. With the argument of national security being invalid, the directive would contradict with the right for information privacy, which would make it illegal in further consequence.

On 8 April 2014 the *Court of Justice of the European Union* came to this conclusion and nullified the *Data Redemption Directive*, because of human right violation [3].

6 Closure

At the example of the Data Retention Directive we observe that making laws and judging legal aspects regarding the internet is a hard thing to achieve. Because of the wide interconnection of people in different countries, with most of these countries having their own and part wise drastically different [5] data protection laws, complete internet privacy is long gone.

References

[1] http://conventions.coe.int/treaty/en/Treaties/Html/005.htm

[2] http://firstmonday.org/ojs/index.php/fm/article/view/2611/2302

[3] http://malte-spitz.de/wp-content/uploads/2013/12/CP130157EN.pdf

[4] http://en.wikipedia.org/wiki/Information_privacy_law

[5] http://en.wikipedia.org/wiki/Information_privacy_law#.22Safe_Harbor.22_Privacy_Framework

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[8] http://www.oecd.org/sti/ieconomy/privacy.htm

[5] e.g.: China