LEGAL AND PRIVACY CHALLENGES OF SOCIAL NETWORKING SITES

Facebook

University of Oslo

Faculty of Law

Candidate number: 525223

Supervisor: Professor Lee A. Bygrave

Deadline for submission: ….. (12/01/2011)

Number of words: 16,633 (max. 18.000)

22.05.2012

Content

1 Introduction

Information and communication technologies are part of our everyday life. On one hand their development is beneficial for the overall wellbeing of the society we live in, whereas on the other legal issues emerge with respect to their utilization and application.

Social networking sites are one of these recent developments that appeared with the Web 2.0 boom and are becoming more and more popular nowadays. The most prominent of them is Facebook[1] with a mission to give people the power to share and make the world more open and connected, keep up with friends, upload an unlimited number of photos, share links and videos, and learn more about the people they meet.[2] LinkedIn (a business-related, professional network)[3], Hi5 (a social play network)[4] and Twitter (a real-time information network that connects people to the latest information about what they find interesting)[5] are some of the other well-known social networking sites.

The number of users of social networking sites is increasing constantly. They are attracting huge numbers of users on a daily basis. According to a document presented by Goldman Sachs Group Inc., a global investment banking and securities firm, as of January 2011 Facebook has more than 600 million active users.[6] The Facebook founder, Mark Zuckerberg, announced in July 2010 that the number of Facebook active users crossed 500 million users.[7] LinkedIn has published that as of March 2011 it has more than 100 million users worldwide.[8]

---

[1] Facebook was initially intended to be a social network of university and college communities. Purportedly, it owes its main success to the wide acceptance among university students. Other reasons are the amount and the quality of personal information users share on it and the fact that this information is personally identified.
[2] Facebook Homepage <http://www.facebook.com/facebook?sk=info> last accessed 10.11.2011
[3] LinkedIn Homepage<http://www.linkedin.com/static?key=what_is_linkedin&trk=hb_what> last accessed 10.11.2011
[4] Hi5 Homepage <http://www.hi5networks.com/> last accessed 10.11.2011
[5] Twitter Homepage <http://twitter.com/about> last accessed 10.11.2011
[6] Nicholas Carlson, 'Facebook has More than 600 Million Users, Goldman Tells Clients' *Business Insider* (5th Jan. 2011) <http://www.businessinsider.com/facebook-has-more-than-600-million-users-goldman-tells-clients-2011-1> last accessed 17.11.2011
[7] M Zuckerberg, '500 Million Stories' *The Facebook Blog (*21 July 2010) <http://blog.facebook.com/blog.php?post=409753352130> last accessed 17.11.2011
[8] http://press.linkedin.com/about/ last accessed 17.11.2011

The immense number of users these social networking sites attract has brought in many questions as to whether they are appropriately legally regulated and how they ought to be regulated in the near future.

This thesis will discuss the legal issues emerging from the mass utilization of social networking sites with in-depth analysis in particular of the privacy concerns raised. For this goal, the relevant European Data protection legislation will be examined in more detail with special emphasis on the provisions that can be related with social networking sites.

Chapter 4 and 5 of this Thesis will examine respectively the question who can be data controller in the context of social networking sites and the applicability of the European data protection laws to social networking sites not established within EU. Chapter 6 and 7 will analyze the privacy concerns and the legal issues related with the users and the social networking sites themselves, such as ownership and control over the content of the material published on the sites and the liability of social networking sites resulting from the publication of information provided by third parties. Chapter 8 will discuss the proposed reformes in the European data protection legislation. Finaly, Chapter 9 will conclude.

2 The notion Social Networking Sites

Boyd and Ellison define social network sites as web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system.[9]

The Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data[10] established pursuant to Article 29 of the Data Protection

[9] D Boyd, N Ellison, (2007) 'Social network sites: Definition, history, and scholarship' *Journal of Computer-Mediated Communication*, *13*(1), article 11.,<http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html> last accessed 18 Nov. 2011

[10] The Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data is an independent advisory body on data protection and privacy that analysis the application of the EU Directives on data protection with the goal of contributing to their uniform application. The Article 29 Working Party can issue recommendations, opinions or working documents. It is composed of representatives from the

Directive defines social networking services as online communication platforms which enable individuals to join or create networks of like-minded users[11] and further clarifies that they are information society services.[12] According to the Article 29 Working party, common characteristics of the social networking services are the invitation of the users to provide personal data for the purpose of generating a description of them (profile), the existence of tools which allow users to post their own material (a photograph, music or video clip or links to other sites) and the creation of list of contacts for each user with which users can interact, thus enabling social networking.

While Boyd and Ellison define the social networking websites as web-based services the Article 29 Working Party defines them as online communication platforms. In the other parts the definitions overlap. For the purposes of this thesis the definition of the Article 29 Working Party will be accepted for defining the social networking websites, as online communication platforms on which users publish various types of information.

Typically, the personal data users publish include the user's name, sex, birthday, age, and contact information such as e-mail address, instant messenger screen name, telephone number, and address. Depending on the social networking site, users may also be able to post their sexual orientation, where they work or attend school and their religious and political affiliation.[13]

The core of the social networking sites is composed of users' profiles showing an expressed list of users' friends who are network users as well. The basic idea is that members will use their online profiles to become part of an online community of people

---

national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission. Pursuant to Article 30 of the Data Protection Directive it advices the Commission on any proposed amendment of the Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms. For further details, see Pulet, Y and Gutwirth, S (2008) The Contribution of the Article 29 Working Party to the Construction of a Harmonised European Data Protection System: An Illustration of "Reflexive Governance"? In Perez Asinari, M.V. and and Palazzi, P. (eds.), *Défis du Droit à la Protection de la Vie Privée / Challenges of Privacy and Data Protection Law*, Bruylant, Brussels, pp. 569–609.

[11] Article 29 Data Protection Working Party: Opinion 5/2009 on online social networking (WP 163) (June 12, 2009), p.4. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf>

[12] Information society services are defined in the E-Commerce Directive (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ 17.07.2000, L178/1) as any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of the service.

[13] B Henson, B Reyns and B Fisher, (2011) 'Security in the 21st Century: Examining the Link Between Online Social Network Activity, Privacy, and Interpersonal Victimization' *Criminal Justice Review*, 36(3) p. 1-16, 4

with common interests.[14] The term 'friends' in the context of social networking sites does not have the same meaning as the relationship that sociologists would generally recognize as friendship in other dimensions of life. Rather it is used to indicate a consensual connection between two users.

Users can also control with whom they want to link their account by sending and accepting a friend request. The visibility of a profile varies by site and according to user discretion.[15] Users can shield their profiles by using the privacy settings and restricting access to whole or part of their profile to chosen contacts. Other users can see the content of a users' profile only if the user has set the privacy settings of his profile to public. If the user has set the privacy settings of his profile to private, then only friends can view that person's profile information. Nevertheless, the privacy of the users who will not change the default privacy settings is to a large extent in the hands of the providers of the social networking services.[16]

For example, Facebook allows users who are members of the same network to view each other's profiles, if the profile owner has not denied access to his profile to the network members. Facebook provides its members with the possibility to control the privacy of their personal information by limiting the visibility and searchability of the profile. However by default participants' profiles are searchable by anybody else on the Facebook network, and actually readable by any member at the same college/university and geographical location.[17]

Therefore, the Article 29 Working Party has recommended that social networking sites should offer privacy-friendly default settings which allow users to freely and specifically consent to any access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties.[18]

In my view, the default settings of the social networking websites should be based on opt-in procedure, i.e. the profile visibility from the outset should be set to private and the user should decide what data to reveal instead of being obliged to opt-out as it is now.

---

[14] *Doe v. MySpace, Inc.,* 474 F.Supp.2d 843, 845-846 (W.D. Tex. 2007)
[15] Boyd, Ellison (n 9)
[16] E Kosta, (2010) 'The Freddi Staurs of Social Networking – A Legal Approach' in M. Bezzi et al. (Eds.): *Privacy and Identity* (IFIP AICT 2010) pp. 66–74, p. 67.
[17] A Acquisti, R Gross, (2006) 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook' Proceedings of 6th Workshop on Privacy Enhancing Technologies, Lecture Notes in Computer Science 4258, *Springer*, 36-58
[18] Article 29 Data Protection Working Party (n 11), p.7

Viviane Reding, the EU Justice Commissioner, in a speech on the ongoing review of the EU data protection framework has stressed the need to build peoples' data protection rights on four pillars: the right to be forgotten, transparency, data protection regardless of location and privacy by default.[19] She reiterated that privacy settings often require considerable operational effort in order to be put in place and are not a reliable indication of consumers' consent. For these reasons a "privacy by default" rule needs to be introduced, which would also be of use in cases of unfair, unexpected or unreasonable processing of data, when data is used for purposes other than for what an individual had initially given his or her consent or permission or when the data being collected is irrelevant.[20]

Most of the social networking websites provide their users with the possibility to send messages, photos and attachments to users who are on their friend list. Some of them even allow users to send messages to other user who are not listed as their friends.

By default, every user's profile includes an area in which other users can post public messages (a "Wall"). These messages exist on the user's profile until deleted by either the profile user or the user who posted the public message, or until the profile user deactivates his or her Facebook account. Messages posted on a user's wall are not restricted and they may contain text, video, pictures, or links.[21]

Usually users cannot delete all Wall posts with a single click. Rather, they must be deleted one by one. Recently Facebook introduced the possibility to limit the audience for old posts on a users' profile. This tool allows the content on a user profile that was shared on the user Wall with more than the user friends, like public posts for example, to change to Friends. However people who are tagged and their friends may see those posts as well. The possibility for the user stays to individually change the audience of his posts by going to the post and choosing different audience.[22]

Also some social networking websites such as Facebook and Twitter for example have introduced instant messaging systems or chats where users can have real time conversations on the site.

---

[19] Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner (2011) 'Your Data Your Rights: Safeguarding Your Privacy in a Connected World' Speech 11/183, Brussels
[20] Ibid.
[21] P Lawson, (2008) 'Reply to the Canadian Privacy Commissioner regarding the PIPEDA Complaint: Facebook' Canadian Internet Policy and Public Interest Clinic, p. 3
[22] Facebook Homepage http://www.facebook.com/settings/?tab=privacy last accessed 17.11.2011

2.1 Adventages of Social Networking Sites

Social networking sites allow their users to share content which they have produced themselves and receive content from others, which appears to be one of their biggest advantages, to create and share with the world. In addition, they allow users to organize their social or political lives online, to keep in touch with friends and relatives and to discuss ideas and opinions with people living at the other end of the world. Social networking sites encourage self-expression and socialization in a way in-person interaction might not encourage. Also, they create possibilities to meet new people through interaction with existing online friends, membership in an online group or through people searching tools.

Social networking sites have shown to be beneficial to companies and businesses as well, in particular to those who conduct their marketing activities online. They allow companies to develop new marketing strategies and to find out customers' opinions about their products. Also, by gathering valuable information from users they can offer targeted advertising - advertising tailored in accordance to the users' preferences.

Lastly, they are subject to continuous development and creation of new tools which does not entail great investment costs.[23] The modest investments necessary for creation of a social networking site makes it relatively easy for new companies to enter the market and develop their site. This is beneficial from economic point of view in general because it increases competition and brings better quality services to the users.

The European Commission has recognized that social networking sites represent economic opportunities for the European industry, offering at the same time to the society new ways to communicate and express creativity.

[23] European Commission, Information Society Home page http://ec.europa.eu/information_society/activities/social_networking/opps_risks/index_en.htm last accessed 17.11.2011

3 Legal Background for Data Protection in the European Union

Primary points of reference for the current European Union legislative framework for privacy and data protection are two international instruments[24], the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[25], the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[26] and two Directives, namely the European Union Data Protection Directive[27] and the EU Directive on Privacy and Electronic Communications.[28]

Data protection laws regulate the manner in which data identifying individuals or pertaining to them are processed and subjects such processing to a defined set of safeguards.[29] Data protection laws embody all or most of the principles on processing of personal information or personal data.

Personal data are defined as all information relating to an identified or identifiable person, either directly or indirectly. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.[30] The list of principles includes the principle of fair and lawful processing,[31] the principle of minimality,[32] the principle of purpose specification,[33] the principle of information quality,[34] the principle of data subject participation and control,[35] the principle of disclosure limitation,[36] and the principles of information security and sensitivity.[37]

---

[24] LA Bygrave *'Data Protection Law: Approaching Its Rationale, Logic and Limits*' (Kluwer Law International, The Hague / London / New York 2002) chapter 2, p. 30
[25] European Treaty Series No. 108; adopted 28th Jan. 1981; in force 1st Oct. 1985.
[26] Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Paris, 1980)
[27] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31
[28] Directive (EC) 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37
[29] C Kuner, (2010) 'Data Protection Law and International Jurisdiction on the Internet (Part I)' *International Journal of Law and Information Technology* 18(2), 176 -193, p.176
[30] Recital 26 of Directive 95/46/EC.
[31] Data Protection Directive, article 6(1)(a)
[32] Data Protection Directive article 6(1)(c)
[33] Data Protection Directive article 6(1)(b)
[34] Data Protection Directive article 6(1)(d)
[35] See eg. Data Protection Directive article 10-12, Article 14 containing the right to object to data processing
[36] OECD Guidelines, paragraph 10, Use Limitation Principle
[37] Bygrave (n 24) p. 57 - 68

The term data protection is mostly used in Europe. In the United States the term privacy protection is used instead.

The existing laws apply equally to online and offline conduct even though all of them were adopted in a significantly different technological landscape than the one today, where the Internet was not that well known and dispersed.[38] Data protection laws are applicable at any time personal data are processed, therefore they apply to almost any operation performed on the Internet involving processing of personal data, especially nowadays when a new generation of users has grown up that incorporates online technologies into their everyday lives.[39]

3.1 The EU Data Protection Directive

The EU Data Protection Directive establishes a regulatory framework that strikes a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union. The Directive is the key regulatory instrument adopted by the Union institutions to regulate this field.

Even though some of the provision and solutions provided in the Data Protection Directive were highly criticized in the recent years, the main principles of the Directive have set the standard for the legal definition of personal data, regulatory responses to the use of personal data and other innovations in data protection policy.[40]

With respect to the regulation of the social networking sites however it should be kept in mind that the Data Protection Directive was enacted when the internet was in its early stages, before its expansion in Europe and before the web 2.0. The European Commission did not have social networking sites in mind when drafted the Directive. Thus, even though its principles can be applied on the cases involved social networking sites, some issues still remain uncovered.

This was one of the reasons why the European Commission decided to revise the data protection legislation and approached to drafting and preparing a new data protection package. The European Commission published a Consultation on the Commission's

---

[38] O Tene, (2011) 'Privacy: The New Generations' *International Data Privacy Law*, 1(1), p.15
[39] http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf
[40] CJ Bennett, C Raab '*The Governance of Privacy: policy instruments in a global perspective'* (2nd Edition, MIT Press, London 2006) p 97

comprehensive approach on personal data protection in the European Union in November 2010.[41] The aim of the Consultation was to obtain different opinions from citizens, non-governmental organizations, businesses and public authorities on how to address the new challenges for personal data protection in the Union imposed by the fast developing technologies and the globalization. As a consequence, the Commission considered that some kind of action is necessary in order to ensure an effective and comprehensive protection for individual's personal data within the EU.

Viviane Reding, the EU Justice Commissioner, in a speech held on a Conference in London 2011, pointed out the consultations have confirmed that the underlying principles of the current EU data protection legislation are still valid but in any case there is a need for a more comprehensive and more coherent approach in the EU policy for the fundamental right to personal data protection.[42]

4 Data Controllers

The Data Protection Directive provides the definitions for the key terms data processing and data controllers. 'Data processing' is defined as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

The activities of social networking sites (Facebook), namely the collection of users' data and their storage, would fall under the category of data processing operations, as defined in Article 2 of the Directive.

---

[41] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4th November 2010

[42] Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner Assuring data protection in the age of the internet British Bankers' Association Data Protection and Privacy Conference London, June 2011 <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/452&format=HTML&aged=0&language=EN&guiLanguage=en> last accessed 18.11.2011

Definition of data controller is provided in Article 2(d) of the Data Protection Directive, stipulating that data controller is "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data". Controllers must take the appropriate technical and organizational measures, 'both at the time of the design of the processing system and at the time of the processing itself' to maintain security and prevent unauthorized processing, taking into account the risks represented by the processing and the nature of the data.[43]

With respect to social networking websites data controllers can be the social networking service provider, the application providers and arguably the user himself. The role of each of them will be discussed briefly in the following lines.

4.1 Social Networking Sites as Data Controllers

Considering the relevant provision of the Data Protection Directive, social network providers are data controllers with respect to the social networking services. They determine the means for the processing of users' data and the purposes and management of the users' accounts such as the account registration and deletion. Social network service providers also determine the use that may be made of user data for advertising and marketing purposes which includes as well advertising provided by third parties.

As data controllers, social networking sites must follow the data protection principles, in particular principle of fair and lawful processing and they must obtain users consent to process their personal data[44]. Also, they must obtain users explicit consent[45] for processing sensitive personal data about them.

Sensitive personal data is defined in the Data Protection Directive as personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life. The Directive states that particular conditions and safeguards must be observed when particularly "sensitive" personal data is processed.[46]

---

[43] Data Protection Directive, article 17 and Recital 46
[44] Data Protection Directive, article 7(1)
[45] Data Protection Directive, article 8(2)(a)
[46] Data Protection Directive, article 8

However, the exception provided in Article 8(2)(e) of the Data Protection Directive, stipulating that the prohibition for processing sensitive personal data would not apply in case where the processing relates to data which are manifestly made public by the data subject would mean that the social networking sites must not obtain the explicit consent of their users due to the fact that users enter and publish their personal data by themselves. The Article 29 Working party recommended social networking websites to make clear that answering questions relating to sensitive data is completely voluntary if they include in the profile form of the users any such questions.

Some authors claim that Facebook via the Like button can extend its reach beyond its platform and members and can trace non-Facebook members as well. When a non-user visits a site which includes Facebook Connect this application issues a cookie. From that moment when the non-user visits other websites with the Like button a request for the Like button is sent from the Facebook server including the cookie.[47]

In this respect social networking websites act as data controllers for the personal data collected about non-users as well. Also they would be regarded as data controllers for the data collected for non-users published by the social networking users themselves. Namely users make public not only information that pertain to them but also to other people, friends or relatives.

4.2 Application Providers as Data Controllers

Facebook allows developers to create different applications which run on the Facebook platform. Application providers developing applications which run in addition to the ones from the social networking sites can also be data controllers if collecting users' personal data. [48] Generally users are required to give their consent to the application providers to access their personal data when they sign up for the new application, thus entering directly into contractual relations with the application provides. In any case, application providers must abide by the data protection laws and principles when processing users' data.

[47] A Roosendaal, (2010) 'Facebook Tracks and Traces Everyone: Like This!', p.2 Electronic copy available at: <http://ssrn.com/abstract=1717563> last accessed 18.11.2011
[48] Article 29 Data Protection Working Party (n 11).

4.3 Users as Data Controllers

Users are data subjects. However, in the social networks environmental setting individuals can be brought within the scope of the definition of "data controller". Having in consideration the fact that the definition of data controller is very broad, encompassing any natural person who determines the purposes of processing personal data, not only the social networking sites but also their users, individuals who post information about them and their friends might be regarded as data controllers as well.[49]

In order to be qualified as a controller, a user must exercise at least some level of decision-making power with regards to both the purposes and means of a particular processing operation. As to determining the technical means of the processing, the user of a social networking website generally does not have a great deal of decision-making power. The user only acts as a controller with regards to the content he chooses to provide and the processing operations he initiates because he decides when accessing a social networking website what information to upload.[50] What is typical for users on the social networking websites is that they often publish photos with other users and tag them without obtaining prior consent from the tagged users.

In this respect, users would be obliged to comply with the data protection principles of the Data Protection Directive regarding the processing of personal data such as fair and lawful processing (Art. 7 DPD), minimality, purpose specification etc. However, it is unrealistic to expect that all users of a social network will respect the data protection principles enshrined in the Directive and extremely difficult for the Data Protection Authorities to monitor and police users' compliance with the principles.[51]

Therefore, an emerging problem is how to control the invasion of privacy by other users. Significant question in this respect is should the household exemption still apply. Namely, Article 3(2) of the Data Protection Directive stipulates that the Directive shall not

---

[49] R Wong, (2008) Social Networking: Anybody is a Data Controller! Electronic copy available at: <http://ssrn.com/abstract=1271668> last accessed 18.11.2011

[50] V Alsenoy, B Ballet, Joris et al. (2009) 'Social networks and web 2.0: are users also bound by data protection regulations?' available at <http://www.springerlink.com/content/u11161037506t68n/fulltext.pdf >, IDIS 65–79, p.70

[51] D Garrie, R Wong, R (2010) 'Social networking: opening the floodgates to personal data' *Computer and Telecommunications Law Review*, 16(6), 167-175, p. 169

apply to the processing of personal data by a natural person in the course of a purely personal or household activity. [52]

On one hand, it can be argued that for the users on social networking websites the household exemption should apply, as individuals who process personal data in the course of a purely personal or household activity. Also the exemptions under Article 9 of the Data Protection Directive, namely that processing was intended for journalistic, artistic and literary purposes might be applicable as well. In the application of the household exemption account should be paid on the need to protect the rights of other users on the network.

On the other hand some authors hold the view that users cannot benefit from the Article 3(2) household exemption when they post personal information about others on a social networking website.[53]

In the Lindqvist case[54] the European Court of Justice (hereinafter ECJ) held that the act of referring on an internet page to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes processing of personal data wholly or partly by automatic means[55] and such processing of personal data is not covered by any of the exceptions in Article 3(2) of the Data Protection Directive.[56] The reasons behind the decision were that the data were made available to anyone with access on the internet.

The ECJ held that the exception must be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consists in publication on the internet so that those data are made accessible to an indefinite number of people.

The case was about a Swedish woman, Ms. Lindqvist, who worked as a catechist for a parish in Sweeden. In 1998, she set up internet pages on her personal computer to allow parishioners prepare for their confirmation. The internet pages contained personal information about 18 persons in the parish where she described the jobs and hobbies of her colleagues and included some of their telephone numbers. In one case she mentioned that one colleague injured her foot and was working half-time for medical reasons. She did

---

[52] Data Protection Directive, article 3(2)
[53] Wong (n 48) p.5
[54] Lindqvist, C-101/01 [2004] 1 CMLR 20
[55] Ibid. para 27
[56] Ibid. para 48

not obtain the consent of the individuals before posting the information on the website and did not inform the Swedish data protection authorities about the processing of sensitive information.

It could be argued that the ECJ took a narrow approach to the interpretation of Art. 3(2) as applied to the internet. However, the implications of this decision are that a distinction is drawn between private and public access to the internet.[57] Namely individuals should limit the access to their profiles to benefit from the exception.

Pursuant to the Article 29 Working Party the processing of personal data by users in most cases will fall within the household exemption, with the exception of the case where a user has a high number of contacts or when access to a profile is provided to all members within the network.[58]

In my opinion, users should not benefit from the household exception if the privacy settings on their profiles are set to public. The data published by them in this manner will be accessible to anyone having Facebook profile. In the light of the wording of the ECJ decision in the Lindquist case these data cannot be regarded as published in the course of the private life of the individual because they are made accessible to an indefinite number of people.

Users should be able to benefit from the household exemption if the access to their profile is restricted to limited number of people/friends.

5 The Reach of the Data Protection Directive Over the Processing of Personal Data of EU Citizens Carried Out by Social Networking Sites Established in Third Countries

The applicability of the EU Data Protection Directive to social networking sites which headquarters are located in third countries is in particularly relevant in relation to the most popular social networking site, Facebook, which is providing its services from the US,

[57] R Wong, J Savirimuthu, (2008) 'All or nothing: this is the question?: The application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet' *John Marshall Journal of Computer & Information Law*, 25(2), p.8
[58] Article 29 Data Protection Working Party (n 11)

operating as US based company, and which has acquired millions of users and members in the EU. Therefore, for the perspectives of the EU users, it is important to analyze the question of the applicable law in case of an alleged breach of the EU users' data protection rights by Facebook. This is essential because Facebook operates as data controller processing personal data of the EU citizens pursuant to Article 2 of the Data Protection Directive. Also it is important to distinguish whether EU users can rely on their national data protection legislations in the case of privacy infringement.

To answer the question whether Facebook and the other social networking service providers who have their headquarters in countries outside the European Union are also subject to the stricter European data protection rules two provisions of the Data Protection Directive should be looked at in more detail. First the provisions of applicable law contained in Article 4 of the Directive and second through the recourse of Article 25 of the Data Protection Directive. To get better insight in the way these provisions are applied in the real life situations, Facbook will be taken as an example.

It should be taken in consideration that the Article 29 Working Party in its opinion on online social networking expressed the view that the provisions of the Data Protection Directive apply to social networking service providers in most cases, even if their headquarters are located outside of the European area.[59]

5.1 Article 4 of the Data Protection Directive

In accordance with Article 4 of the Data Protection Directive dealing with the applicable national law, each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

> "(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

[59] Article 29 Data Protection Working Party (n 11) p.5.

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."

Pursuant to Article 4, principle criterion for determining applicable law is the data controller place of establishment, irrespective where the data processing takes place. 'Choice of law', 'conflict of laws', or 'applicable law' deals with the question which law or laws shall be applied in a given case.[60] Paragraphs (a) and (c) are based on the so called 'territoriality' principle, meaning that the connecting factor is the location of the controllers.[61] Recital 19 of the Directive clarifies that establishment means "the effective and real exercise of activity through stable arrangements".[62] "The legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect".

The intention behind Article 4 to be drafted the way it is now, according to the preparatory materials of the Data Protection Directive was to avoid the possibility that the data subject might find himself outside any system of protection because the law might be circumvented in order to achieve this and also the same processing operation might be governed by the laws of more than one country.[63]

In order to analyze this provision of the Directive in relation with Facebook it should be determined first where Facebook has its establishment. Pursuant to the information provided on the Facebook webpage,[64] it is headquartered in Palo Alto, California, US and besides the offices it has in US it has international offices in Dublin, Hamburg, London, Madrid, Milan, Paris, Stockholm, Selangor, Singapore, Sydney, Tokyo, Toronto, Hong

---

[60] C Kuner, (2010) 'Data Protection Law and International Jurisdiction on the Internet (Part I)' *International Journal of Law and Information Technology* 18(2),176 – 193, p. 179

[61] L Moerel, (2011) 'The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to processing of Personal Data of EU Citizens by Websites Worldwide?' *International Data Privacy Law,* 2011, 1(1), 28-46, p.29

[62] Data Protection Directive Recital 19

[63] LA Bygrave (2000) 'Determining Applicable Law pursuant to European Data Protection Legislation' *Computer Law & Security Report*, 16, 252–257

[64] <http://www.facebook.com/press/info.php?execbios#!/press/info.php?factsheet> last accessed 17.11.2011

Kong and Hyderabad. On its webpage Facebook has also published that data uploaded by individuals to the Facebook social networking platform are covered by separate notices and by their privacy policy issued to address such situations.[65]

With respect to the application of Article 4(a) on the case of Facebook two situations can be distinguished. In the first situation users are uploading their data on the Facebook website directly to US. This is most probably the way EU citizens' data were stored and processed by Facebook in the early years of its creation. In this case EU data protection laws cannot be applied to protect the data rights of EU residents, because of the jurisdictional issues. EU las and institutions cannot exercise control over the data processing activities of companies established in other countries.

The second situation would be the one where Facebook establishments in Europe are processing data in EU, in the context of their activities, which would have as a corollary Facebook being under the obligations arising from the European data protection laws based on the EU Data Protection Directive. However, information about the exact nature of the activities of the Facebook offices located in Europe and, most important, whether they are involved in data processing is very difficult to obtain.[66] On a question sent to Facebook on 10th of June 2011 through their contact email, asking how Facebook is collecting personal data of EU citizens, whether this data are collected by the Facebook offices in EU (e.g. Facebook Ireland) or are collected directly by the offices in US I received the following answer:

"We apologize for any inconvenience but we are unable to respond to research requests. We encourage you to review our Privacy Policy at http://www.facebook.com/policy.php, which contains additional information that may help you."

In addition, the Danish Data Protection Authority posed the same questions to the Facebooks' Chief Privacy Office in a letter from April 2009.[67] Among the questions raised, the Danish Data Protection Authority asked a question related to jurisdiction issues, namely whether Facebook is established as a data controller in the European Community, if so, in which country if not, whether Facebook is using equipment situated in Denmark

---

[65] <http://www.facebook.com/safeharbor.php> last accessed 17.11.2011
[66] A Kuczerawy (2010) 'Applicable data protection law in a relationship between EU users and non-EU based Social Networking Site' in M. Bezzi et al. (Eds.): *Privacy and Identity* (IFIP AICT 2010), pp. 75–85
[67], J Christoffersen, Danish Data Protection Agency 'Facebook's Processing of Personal Data' 3 April 2009 <http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Facebook.pdf > last accessed 18.11.2011

and if Facebook is collecting personal data in Denmark for the purpose of processing in a country which is not a member of the European Community. Facebook Chief Privacy Officer responded on these questions in June 2009, saying that Facebook is not established as a data controller in the European Community and does not have any equipment in Denmark. However, he acknowledged that Facebook collects information from Danish citizen for processing in the United States and for this processing it gains consent of the Facebook users through their voluntary acceptance of Facebook Statement of Rights and Responsibilities and Privacy Policy.[68]

Despite these responses given by Facebook, in recently drafted Response to the European Commission Communication on personal data protection in the European Union, Facebook has revealed that the Facebook user data is stored in the United States on servers owned or managed by Facebook Inc. but also that the company has a European headquarters in Dublin, Ireland and a subsidiary company, Facebook Ireland Ltd, which is the contracting party for all users of the service in Europe.[69]

The above mentioned statement in the Facebook response to the European Commission Consultation should be taken with due attention. Also, the Facebook Statement of Rights and Responsibilities should be taken into account. Section 18 of the Statement stipulates that for residents and businesses with principal place of business in the US or Canada the Statement represents an agreement between them and Facebook, Inc. Otherwise, the Statement is an agreement between the users and Facebook Ireland Limited. It also states that this Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.[70] Thus, the second situation under article 4 (a) can be deemed relevant as well.

It should be noted that Facebook recently, in April 2011, amended Section 16 of its Statement of Rights and Responsibilities that pertains to the users outside the United States and is titled Special Provisions Applicable to Users outside US. This Section stipulates that Facebook strives to create a global community with consistent standards for

---

[68] C Kelly, Facebook Chief Privacy Officer 'Reply to Danish Data Protection Authority' 11 June 2011 <http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Facebook_Svar.pdf > last accessed 18.11.2011

[69] Facebook Response to European Commission Communication on personal data protection in the European Union prepared by representatives of Facebook Ireland Ltd. and Facebook Inc. <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/facebook_en.pdf> last accessed 18.11.2011

[70] Section 18, Facebook Statement of Rights and Responsibilities, <http://www.facebook.com/terms.php>, last accessed 17.10.2011

everyone and also strive to respect local laws. Users outside the United States consent to having their personal data transferred to and processed in the United States.[71]

The provision of the Directive does not say that the data processing must be carried out by the establishment in a Member State, thus making possible the data processing to take place in the context of the activities of an establishment in a Member State, whereas the actual data processing itself to be carried out by a third party outside the Member State, underlying the long-arm reach of the Data Protection Directive.[72]

With the Facebook example, this will mean that if Facebook in US processes data of EU subscribers in a member State in which it has establishment and this processing is in the context of the activities of this Facebook establishment, then EU data protection laws will be applicable, namely the data protection laws of the respective EU Member State.

Having in consideration the fact that users enter in contractual relations with the Facebook establishment in Ireland, the stricter European data protection laws should be applicable to the Facebook data processing in EU.

5.2 Use of Equipment Situated on the Territory of a Member State of the European Union as Basis for Application of the Data Protection Directive on the Processing of Personal Data – Article 4 (c)

Article 4(c) stipulates that the national law of a member state would apply if the data controller is not established within the EU but uses equipment located on the EU territory for purposes of processing personal data. Recital 20 of the preamble to the Directive provides:

"The fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice; …".

---

[71] Section 16, Facebook Statement of Rights and Responsibilities, http://www.facebook.com/terms.php, last accessed 17.10.2011

[72] Moerel (n 60) p.30

In the recital therefore the term equipment is omitted. On the contrary, the recital operates with the term means used.

Article 4(1)(c) is focused not on the use of equipment per se, but on preventing data controllers from evading EU rules by relocating outside the EU. Thus, Article 4(1)(c) also focuses on the effect produced in the EU by data processing outside the EU, and the protection of EU citizens.[73]

The Article 29 Working Party in its Opinion 5/2009 on online social networking sites expresses the view that the provisions of the Data Protection Directive apply to social networking service providers in most cases, even if their headquarters are located outside of the European area.[74] It referred to its earlier opinion on search engines for further guidance on the issues of establishment and use of equipment as determinants for the applicability of the Data Protection Directive and the rules subsequently triggered by the processing of IP addresses and the use of cookies[75], where it states basically that EU data protection laws will apply if a non EU based search engine makes use of cookies on the territory of the EU.

Thus, the computer of a user is a type of equipment that falls under the provision of the Data Protection Directive and by placing cookies on the computers' hard disk a data controller is processing personal data by making use of equipment situated on the territory of an EU Member State in the light of Article 4(c) Data Protection Directive. This will trigger the application of Member States national laws of the pace where the computer is to be found on the data processing activities.

Considering Article 4(1)(c) in this way gives rise to the possibility of regulatory overreaching in the online environment, meaning a situation in which the rules are expressed so generally and non-discriminatingly that they apply to a large range of activities without having much of a realistic chance of being enforced.[76] In fact, this would lead to a situation where all websites based outside the EU that use cookies will be covered by the Directive and EU Member States national data protection laws. Also, data controllers would be placed in an unfavorable condition by having to comply with the stringent EU data protection laws. One limit of the "cookies" solution is the fact that the

---

[73] Kuner (n 29) , p.190
[74] Article 29 Data Protection Working Party (n 11)
[75] Article 29 Data Protection Working Party: Opinion 1/2008 on Data Protection Issues Related to Search Engines (WP 148)
[76] Bygrave, (n 62) 2000) p. 252–257

user must be notified when the cookie is installed on his computer and if he doesn't agree to that a paradoxical situation could occur in the sense that the user, wishing to protect his privacy by refusing the cookies would in fact deprive himself of the protection by his national data protection law because Article 4(1)(c) applies only if the data controller uses equipment, that is the user's computer, on the territory of the Member State through the cookie.[77]

If the Opinion 5/2009 on online social networking is followed, the provisions of the Data Protection Directive and respectively the national laws of all 27 EU Member States will apply to data processing operations of social networking sites such as Facebook. However, Article 4(1)(c) in its current form does not provide a basis strong enough to ensure the protection of the European data subjects in the context of social networking sites and does not provide legal certainty.[78]

The primary goal Article 4(c) serves is to protect EU citizens form their data being processed by data processors outside the control of EU law, not offering an adequate level of protection to the one established in EU. Also, it serves to prevent the avoidance by data controllers to fulfill their obligations under the Directive by transferring their establishment in non-EU Member Country. Even if the overreaching effect this provision might create might seem justifiable from the perspective of an EU citizen, in my view it will go too far to extend the application of the EU data protection laws on social networking websites on the bases of installing cookies on users' computers. In addition, it would be very difficult, if not impossible to enforce the provision.

5.3 Transfer of Personal Data pursuant to Article 25 of the Data Protection Directive

Pursuant to Article 25 of the Data Protection Directive transfer of personal data to third country may only take place if the third country in question ensures an adequate level of protection. Thus, by requiring third countries to provide adequate level of protection to that applied in EU, EU can extend the reach of its data protection laws to countries outside its

[77] Kuczerawy (n 65) p. 81
[78] Ibid.

boundaries. The Commission has the power to determine on the bases of Article 25(6) whether a third country ensures an adequate level of protection.

The US policy of self-regulation of organizations within the scope of data protection does not provide a level of protection of personal data comparable to European standards. The adequacy test has not been applied to US (where Facebook and many of the other social networking sites have their headquarters) in the manner envisaged with the Directive, with formal decision on adequacy by the Commission. However, in order not to restrict the flow of data between EU and US, the two major world economic players, they entered in Safe Harbor Agreement, as laid down in the Commission Decision 520/2000/EC,[79] allowing US businesses to transfer data to US if they comply with the principles set in it. Companies that self-certify to comply with the Safe harbor principles can transfer data from EU to US without being subject to "the adequate level of protection" criterion. Also, in case of dispute, if an EU citizen claims his privacy rights have been infringed, US law will apply and the case will be heard before US dispute resolution bodies.

Facebook as a company with headquarters in California has self-certified that adheres to the Safe Harbor Privacy Principles published by the US Department of Commerce[80] which can be interpreted as an attempt to avoid the application of the European Data Protection laws to its data processing activities, because as company that has self-certified compliance with the Safe Harbor principles can transfer users data without being subject of the adequacy criterion. Facebook user data is stored in the United States on servers owned or managed by Facebook Inc. Facebook Inc has a comprehensive registration Under the EU-US Safe Harbor scheme for its processing of data from European users.[81]

On its webpage Facebook has published that the Safe Harbor Notice applies to EEA data relating to data subjects residing in the EEA that Facebook receives and processes, except personal data that are received in the context of employment with a

---

[79] Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce [2000] OJ L215/7

[80] <http://www.facebook.com/safeharbor.php> last accessed 17.11.2011

[81] Facebook Response to European Commission Communication on personal data protection in the European Union prepared by representatives of Facebook Ireland Ltd. and Facebook Inc. <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/facebook_en.pdf> last accessed 17.11.2011

Facebook company and except data that individuals upload to the Facebook social networking platform.[82] Regarding the categories of data, they include information related to individual independent contractors, and employees and individual representatives of companies and other organizations that do business with Facebook, such as advertising customers.

Also, Facebook provides data processing services to affiliated and unaffiliated entities, including Facebook Ireland Ltd., and in that context processes information that such entities instruct to process, on their behalf and subject to their direction. So in this case facebook would not act as data controller, but as data processor. When EEA data is sent to Facebook by another company in the EEA for processing purposes, the categories of data sent and the purposes of processing depend on such other company, the data controller. [83]

Article 25 of the Data Protection Directive applies only to data controllers that collect data in EU and are located within the Union. Therefore, Facebook needs to adhere to the Safe Harbor Principles only if is transferring personal data collected in the EU. Facebook states that Safe Harbor does not apply to data processing via the Facebook platform, which is covered by separate notices issued to address such situations. If local office, branch or subsidiary of Facebook collects data in EU that would have as a corollary Facebook being under an obligation of Safe Harbor. The decision to opt out for the Safe Harbor program does not mean that it committed to comply with the EU Data Protection law.[84] In this case transfer of data does not occur, data are uploaded on the Facebook platform and collected directly by the establishment in US, therefore the Article 25 cannot be applied.

Art. 29 Working Party in its Opinion about the level of protection provided by the Safe Harbor stated that the program does not affect the application of Article 4 of the Directive.

Among the other issues that the ECJ had to consider in the Lindquist case, was also whether Mrs. Lindqvist's behaviour was in breach of Article 25 of the Data Protection Directive. However, the Court held that there is no transfer of personal data to a third country within the meaning of Article 25 of the Directive where an individual in a Member

---

[82] <http://www.facebook.com/safeharbor.php> last accessed 17.11.2011
[83] <http://www.facebook.com/safeharbor.php> last accessed 17.11.2011
[84] Kuczerawy (n 65)

State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.[85] The Court started its reasoning by explaining that the Data Protection Directive does not contain provision concerning use of the internet and in particular, it does not lay down criteria for deciding whether operations carried out by hosting providers should be deemed to occur in the place of establishment of the service or at its business address or in the place where the computer or computers constituting the service's infrastructure are located. Because of the absence of criteria applicable to use of the internet, one cannot presume that the Community legislature intended the expression transfer of data to a third country to cover the loading, by an individual in Ms. Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them.[86]

Nevertheless, there have been suggestions that sites should be subject to liability for invasion of privacy if they do not take down expediently on complaint.[87]

6 Social Networking Sites – Potential Treat to Users Privacy

One of the major concerns arising out of the increased popularity and utilization of the social networking sites is the potential threat to users' privacy. Social networks users publish various types of personal information online. This information linked with the activities of the user and his communications with other users can be used for construction of a person's profile, particularly in regard to that person interests and preferences. Thus the user is exposing him/her to the risk of identity theft.

In most cases users' personal pages are also searchable from any search engine. Users' names can be "googled" and are vulnerable to hackers, solicitors, and scammers.

---

[85] Lindquist, para 71
[86] Lindquist, Para 67 and 68
[87] L Edwards, (2009) 'Privacy and Data Protection Online: The Laws Don't Work?' in L Edwards, C Waelde (ed) '*Law and the Internet'(* Third Edition, 2009, Hart Publishing) pp.443-488, p.479

As previously mentioned, the personal data can be used for commercial purposes by advertisers offering targeted advertisements based on the information revealed by the user.

As pointed out before, users often without knowing do not restrict their profiles visibility to friends only and leave their profiles open to public audience. The default settings of most of the social networking websites are privacy invasive. They require users to publish certain data that relate with their personality and privacy.

Other feature of the social networking sites which has as a consequence intrusion of users privacy is the possibility to create groups or networks of users based on shared ethnic or geographical origin, educational background, political views etc. This feature of the social networking websites allows more information about one user to be publicly revealed and gathered. Another feature having the same consequence is the possibility to access on a user profile through mobile phones and make public the location of the user.

In addition, typically the social networking websites preserve the right to unilaterally amend their terms of use at any time which allows flexibility for them to alter their business model and terms of business without needing to contact and agree terms with each user. On a long run, this can undermine any long-term reassurance as to how the content published on the website might be used.[88]

Another worrying aspect of the social networking websites is the fact that they are more and more often used by employers and other institutions as a means to screen applicants.[89]

Because of all these issues social networks are challenging the legal conceptions of privacy and security, both in Europe and US. The European Commission has expressed a concern that social networking sites raise new issues with regard to privacy and the protection of minors, cyber-bullying including harassment that can involve the circulation of photographs, rumors or gossip, exposure to harmful content such as pornography or sexual content, violence, or content inciting to self harm (suicide, eating disorder, etc).[90]

As part of the European Comission Safer Internet Plus Programme, in February 2009, the leading social networking service providers in consultation with the European

---

[88] Ibid.

[89] See eg J Shepherd, D Shariatmadri 'Would be students checked on Facebook', *Guardian,* 10 Jan. 2008 available at <http://education.guardian.co.uk/universityaccess/story/0,,2238962,00.html> last accessed 14.11.2011

[90] <http://ec.europa.eu/information_society/activities/social_networking/index_en.htm>

Commission developed a set of Safer Social Networking Principles for the EU with a goal to enhance the safety of children and young people using their services.

The third principle requires social network service providers to employ tools and technologies to assist children and young people in managing their experience on their service, particularly with regards to inappropriate or unwanted (but not illegal) content or conduct.

The measures that can help minimize the risk of unwanted or inappropriate contact between children and young people and adults may include for example: taking steps to ensure that private profiles of users registered as under the age of 18 are not searchable; setting the default for full profiles to 'private' or to the user's approved contact list for those registering under the age of 18 (some service providers set the profile default as 'private' for all users); ensuring that setting a profile to private means that the full profile cannot be viewed or the user contacted except by 'friends' on their contact list (users may actively choose to change their settings to public or equivalent); giving users control over who can access their full profile by, for example, being able to block a user from viewing their profile and 'reject' friend requests;[91]

6.1 Facebook and the Potential Treats to Users Privacy

The major social networking websites in general undertake measures to comply with the data protection legislation. Their principle mechanisms for compliance are obtaining the consent of all users for the use of their personal data at the point of account opening, having detailed privacy policy setting out how the data will be used, applying privacy settings which allow users to restrict who can view their data and ensuring security of the data on the website to prevent unauthorized access.[92]

However, there are numerous examples of social networking sites actions that have the potential to infringe users' privacy. I will concentrate my discussion on several of them taking the example of Facebook. As previously discussed, Facebook as social

[91] <http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf >
[92] N Graham, H Anderson, (2010) 'Are individuals waking up to the privacy implications of social networking sites?' *E.I.P.R.* 32(3), 99-103, p.99

networking site is data controller and the Data Protection Directive applies to its activities. Therefore Facebook must complies with the strict European data protection laws.

6.2 Applications

Facebook allows developers to create different applications that would run on the Facebook platform and collect users' personal data. In general, users are required to give their consent to the application providers to access their personal data at the moment when they sign up for the new application. Thus users directly enter into contractual relations with the application provides. However, the personal information these application providers collect is far beyond the purpose for which they have been collected, covering almost everything the user has published on his or her profile and information about user's friends.

Actually, when users decide to use an application and give consent to the application providers to access their personal data, they are not informed about the purposes for which the data will be used. Thus the principles of purpose specification of the Data Protection Directive, minimality, as well as fair and lawful processing are infringed.

Facebook requires these third parties to enter into contractual obligations to respect users' privacy before allowing the platform applications onto the website and takes general technical security measures, but does not guarantee the compliance of the third parties.[93]

A possible solution to this problem would be if the access of application providers to users' personal data is limited to only that information actually necessary for the functioning of the application. For example, it is not necessary for the application "Sites I Have Visited" to collect a list of users' friends as it is doing now. Facebook should exercise control over the amount of information collected by the application providers and should develop some kind of technical means to limit the access to users' data.

In addition, these application providers can be located anywhere in the world. Thus, if data of EU citizen are collected, there can be a transfer of personal data and the

[93] Ibid.

provisions of Article 25 of the Data Protection Directive should be applied. Pursuant to this Article, the transfer of personal data to third country may only take place if the third country in question ensures an adequate level of protection. It is questionable whether this is always the case with the application providers. Stricter control should be imposed on the application providers in order to be insured that they transfer data in accordance with the European data protection laws. Facebook should undertake responsibility as well because it allows access to the application providers to the users' data.

6.3 Tagging

In December 2010 Facebook introduced new feature, tag suggestions. When Facebook user uploads new photos Facebook uses face recognition software to match the newly uploaded photos to other photos people are tagged in and suggests the name of the friend in the photos.

According to the Hamburg Data Protection Authority this face recognition feature could infringe EU and German data protection laws because it requires storing a comprehensive database of the biometric features of all users. Also, biometric data should be stored with the subject's express consent and the user should be asked in advance if he wants his data to be stored or not. The current Facebook practice is not in compliance with this requirement. Facebook gives users only the possibly to opt-out. For these reasons the German authorities required Facebook to disable the automatic tagging software (August 2011).[94]

Facebook however had the view that the tagging feature complies with the EU laws. At the time of its introduction one of the Facebook engineers, Justin Mitchell, wrote on the Facebook blog that if for any reason a user doesn't want his name to be suggested he will be capable to disable suggested tags through the Privacy Settings by clicking on "Customize Settings" and "Suggest photos of me to friends." After that, that user name will no longer be suggested in photo tags.[95]

According to Facebook the users' privacy is respected; the suggestions are given on the bases of photos already uploaded by the users on Facebook and users can control

---

[94] C Farivar 'Facebook violates German law, Hamburg data protection official says' *Deutche Welle,* 02 Aug. 2011 < http://www.dw-world.de/dw/article/0,,15290120,00.html> last accessed 19.11.2011

[95] J Mitchell 'Making Photo Tagging Easier' *The Facebook Blog* (30 June 2011) <http://www.facebook.com/blog.php?post=467145887130> last accessed 19.11.2011

what is published, i.e. the tags are only created when the user clicks on the submit button. Thus the user can review and reject any tag.

EPIC[96], along with several privacy organizations, filed several complaints as well with the Federal Trade Commission in the United States about Facebook's automated tagging of users, changes in Privacy settings, and transfers of personal data, stating that Facebook's practices have been unfair and deceptive. As a response to these complaints Facebook undertook actions to address some but not all of the issues that have been raised by the consumer organizations and the complaint at the Federal Trade Commission are still pending.[97]

The issue has not been resolved yet with the German Data Protection Authorities as well. Recently, at the beginning of November 2011, Hamburg's state data protection authority said that it is preparing legal action against Facebook for the company's use of automatic facial recognition features, and further negotiations with Facebook are useless.[98]

In my view, Facebook should required users' prior consent for storing their biometrical data and for the subsequent use of these data. The mere fact that you upload photo one day and the application recognizes you among all the people on the photo is terrifying, showing how much of our privacy we have gave up just by joining a simple social network.

Also, the tagged persons are not given a possibility to decide if they want to be tagged in a photo. It is up to the user uploading the photo to decide. There are numerous situations in which users would not want to be recognized. There might be situations in which someone is caught on a photo by occasion, and would be recognized and tagged if is a Facebook friend with the uploader of the photo. Therefore, there is no consent of the data subject to this processing. Users should at least receive tag suggestions, and then have the possibility to accept or reject the tag suggestion.

Also the principle of proportionality should be taken in consideration as well. Namely, the justification given by Facebook for the introduction of this application, i.e. to

---

[96] EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.
<http://epic.org/epic/about.html> last accessed 19.11.2011

[97] EPIC Homepage 'Facebook's Privacy'< http://epic.org/privacy/facebook/> last accessed 19.11.2011

[98] C Farivar 'Hamburg Considers Suing Facebook over Facial Recognition Feature' *Deutche Welle,* 10 Nov. 2011 < http://www.dw-world.de/dw/article/0,,15523030,00.html> last accessed 19/11/2011

make photo tagging easier for users, is not proportionate to the purpose for which data are collected. The principles of minimality, purpose specification and fair and lawful processing enshrined in the Directive are infringed.

With the latest changes of the Facebook privacy policies if a user doesn't want Facebook to suggest that friends tag him when photos look like the user, he can turn off this feature through the privacy settings on the account menu, by choosing How Tags Work and after Tag Suggestions. However, even if the Tag Suggestions is disabled, friends will still be able to tag photos of the user manually. Disabling tag suggestions will result in the deletion of the user's photo-comparison data that Facebook uses to make tag suggestions work.[99]

In any case, users can only opt out of using this feature, i.e. to remove the tag after a photo has been published and the user tagged. The better solution would be if they are given a chance to opt-in.

6.4 Tracking of Users through the Like Button

Another major concern arose recently related with Facebook. It became public that Facebook tracks its users regardless of the fact that they have signed out of the Facebook page. Namely, the Australian blogger Nick Cubrilovic posted on his blog on 25/09/2011 that even if users are logged out, Facebook still knows and can track every page the user visits and the only solution is to delete every Facebook cookie in the browser, or to use a separate browser for Facebook interactions. Logging out of Facebook only de-authorizes the browser from the web application. A number of cookies, including users account number are still sent along to all requests to facebook.com.[100]

In other words, some of the cookies remain on the computer even after the user loges out, thus whenever the user visits a site that provides link to Facebook by for example "Like" button, information from those cookies is sent back to Facebook, providing a record of what pages the user has visited on the Web. Some authors claim that the "Like" button is also used to place cookies on the user's computer, regardless whether a

[99] http://www.facebook.com/help/tagging last accessed 19/11/2011

[100] Cubrilovic, Nik 'Logging out of Facebook is not enough' *New Web Order* (25 Sep. 2011) <http://nikcub.appspot.com/logging-out-of-facebook-is-not-enough> last accessed 18.11.2011

user actually uses the button when visiting a website which allows Facebook to track and trace users and to process their data. It also allows non-Facebook member to be traced via the Like button.[101]

The tracking of users over the web facilitates profiling. On the basis of the interests revealed by the web users they can be targeted for personalized advertisements. This is actually behavioral targeting, involving tracking of individuals' online activities in order to deliver tailored advertising. The more finely tailored the ad, the higher the conversion or 'click through' rate, and thus the higher the revenues of advertisers, publishers, and various intermediaries.[102]

Two days after, Cubrilovic wrote on his blog that they worked together with Facebook to solve this issue and the cookie that identifies users ID will be destroyed on logout. However, other cookies will remain on the browser, such as the datr cookie that according to Facebook helps them identify suspicious login activity and keep users safe by flagging questionable activity like failed login attempts and attempts to create multiple spam accounts.[103]

Despite the change Facebook has made as a response on the Cubrilovic discovery, the fact remains that up until now Facebook was tracking users whenever they visited a webpage. The privacy concerns of this practice arise because the data collection takes place without the individual web users even being aware, thus the processing takes place without users consent for the data collection. There is no explanation which data is gathered in this manner and to what extent they have been used. Once again, this practice of Facebook is in breach of the principles of fair and lawful processing and Article 6(1)(a) of the Data Protection Directive, the purpose specification of Article 6(1)(b) and minimality and should be sanctioned by the Data protection Authorities.

Also, the activities of the social networking websites need to be more transparent. They should clearly reveal all the activities they perform with regard to users' personal data, while data protection authorities should perform stricter scrutiny on these activities.

Transparency is a concern as well for the Commission. Individuals must be informed about which data is collected, for what purposes and how it might be used by third parties. The EU Justice Commissioner Viviane Reding has stressed the need for

---

[101] Roosendaal (n 47) p.2
[102] Tene, (n 38) p.17
[103] Cubrilovic (n 98)

greater clarity when signing up to social networking because unfavorable conditions such as restricting control of users over their private data or making data irretrievably public are often not clearly mentioned.[104]In addition, the social networking websites constantly introduce new features and applications with the potential to infringe users' privacy due to the fact that these applications are usually developed and controlled by third parties, not the social networking site itself. This brings into play issues of control of and access to the personal data of users by parties other than the social networking site owner.[105]

6.5 Data Deletion

Lastly, data disclosed on Facebook can exist in perpetuity and cause consequences that could not be predicted at the moment when they were published.

Max Schrems, 24 year old law student from Vienna obtained a CD from Facebook with all the personal information kept about him by Facebook. When he printed the document from the CD he got 1222 pages of material about him, including personal messages and chats he deleted more than year ago, pokes dating back to 2008, invitations he has never responded, wall posts he has deleted and hundreds of other details. The messages and posts were marked as deleted on the file but still exited there.

He published a video David and Goliath struggle with Facebook.[106] In addition, he filed 22 complaints to the Irish Data Protection Authority.

The fact that Facebook keeps everything users post on their profile even after they delete it is obviously performed without obtaining users consent, contrary to the principles of processing personal information enshrined in the Directive and to the EU Laws requiring data to be kept only for a limited time. Namely the Data Retention Directive Article 6 stipulates that Data are retained for periods of not less than six months and not more than two years from the date of the communication.[107] This practice of Facebook must be sanctioned by the Data Protection Authorites (in Ireland due to the fact that Facebook's

---

[104] Reding, Viviane, Vice-President of the European Commission, EU Justice Commissioner "Your Data Your Rights: Safeguarding Your Privacy in a Connected World" Speech 11/183, Brussels, 2011

[105] L Edwards, I Brown, (2009) *Data Control and Social Networking: Irreconcilable Ideas?* In Matwyshyn, A. (ed.) Harboring Data: Information Security, Law and the Corporation, Stanford University Press, pp. 202-227, p. 210

[106] http://www.youtube.com/user/europevfacebook#p/c/8ED10AB2E76CD62E last accessed 11/11/2011

[107] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54

establishment in Ireland enters into contractual relations with European users). Facebook should be monitored and obliged to comply with the data protection laws.

7 Other Legal Issues

Privacy concerns are not the only problem raised by the use of social networking sites. There are many other legal issues emerging as well, one of which is the infringement of intellectual property rights. Section 2 “Sharing Your Content and Information” of Facebook’s Statement of Rights and Responsibilities, governing its relationship with users and others who interact with Facebook, provides that for content covered by intellectual property rights, like photos and videos ("IP content") the user specifically gives Facebook a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that the user posts on or in connection with Facebook ("IP License"). This IP License ends when the user deletes the IP content or his account unless the content has been shared with others, and they have not deleted it.[108]

These very broad rights acquired by the social networking websites are similar to ownership. Users have very little control over how their data may be used by the relevant social networking website or any third party to whom it sub-licenses, and if there is no express restriction on the purposes for which the social-networking site can use the content as usually is the case, the data might be used for commercial exploitation.[109]

Users should also be aware of the fact that postings of texts and photos on social networking sites can evidence activities breaching one country laws or organizational (e.g. university, office etc.) rules. This raises the question whether social networking sites should be regarded as a private space where the user has reasonable expectations of privacy or a public space. If they are to be treated as private space where the user has reasonable expectations of privacy, then the utilization of users’ posts and photos as evidence in proceedings against him would arguably breach his privacy.

---

[108] http://www.facebook.com/terms.php last accessed 17.11.2011
[109] Graham (n 91) p.99

Different would be the outcome if the social networking sites are treated as public space, where it will be questionable whether privacy would be protected. In the US *Katz*[110] case the Supreme Court held that a right to privacy exists where an individual has a reasonable expectation of privacy and that protection should be granted to people not places. Some scholars question the possibility of applying the interpretation of the Court of the Fourth Amendment based on the statements of the *Katz* case in a manner that protects citizens from warrantless police searches to address social network sites, namely the rights of police to access content posted to Facebook without a warrant.[111]

In my opinion, if the user has not changed the privacy settings of his profile and has left it open to the public, then he cannot expect that the content of the published material will be regarded as private. This can be compared as making an announcement in a room full of people. One cannot expect that his words will remain among those people without any consequences and in particular if infringing the laws. In the other case, where the user has shield his profile, the content should be regarded as a private space, where the user enjoys reasonable expectations of privacy, however the type of infringement or criminal action should be taken in consideration as well.

The European Court of Human Rights also has been in the process for some years of recognizing that privacy rights do exist even in public spaces, and even where celebrities make themselves accessible to press attention in public.[112] An example of these recent developments is the recent ECHR case of *von Hannover*.

In addition, if users are regarded as data controllers and if the household exemption applies to them, they might still be liable according to general provisions of national civil or criminal laws in question (e.g. defamation, liability in tort for violation of personality, penal liability). Namely only the Data Protection Directive does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity, but the other laws still apply, such as tort or criminal law.

With the growth of users generated content websites (hereinafter UGC) such as the social networking websites, the division between hosting service provider and a content provider is not straightforward. The social networking websites provide a platform on which users post text and photos, they are not required to pay fees for using the

---

[110] Katz v United States, 389 U.S. 347 (1967)
[111] M Hodge, (2006) 'The Fourth Amendment and privacy issues on the "new" Internet: Facebook.com and MySpace.com.' *Southern Illinois University Law Journal*, 31, 95-122. p.121
[112] Edwards, Brown (n 104) p. 210

platform, but the social networking websites derive revenues from selling the users data to companies or by offering different types of advertising. Arguably, the platform providers should be jointly responsible for the content published because they make profits and because they are aware that some of the content published is illegal, which is the "constructive knowledge" with respect to civil liability of Article 14 of the Electronic Commerce Directive.[113]

Article 14 of the Electronic Commerce Directive[114] regulates the hosting services provided by intermediary service providers and stipulates that the intermediary service providers will not be liable for the information stored at the request of the recipient of the services under the condition that the provider does not have actual knowledge of the illegal activity or information, with regard to criminal liability, and with respect to civil liability, the provider is not aware of facts and circumstances from which the illegal activity or information is apparent – the constructive knowledge requirement.

Also, upon obtaining awareness or knowledge that a content published on the web platform is illegal, the social networking service provider should act expeditiously to remove or disable access to the illegal content (notice and takedown procedure) in order to benefit from a limitation of liability. The removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level.[115]

The example of the French MySpace decision of 22 June 2007[116] shows that social networking websites can be held liable for copyright rights infringements. In the case a French cartoonist whose sketches had been posted without prior authorization successfully sued MySpace for infringement of his author's rights and personality rights. The The Tribunal de Grande Instance de Paris in a summary order found that MySpace should be classified as a publisher not as host because it provided "a presentation

---

[113] L Edwards, Lilian (2009) 'The Fall and Rise of Intermediary Liability Online' in L Edwards, C Waelde (ed) "*Law and the Internet*" (Third Edition, Oxford, Hart Publishing, 2009), p.67

[114] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce) [2000] OJ L178/1.

[115] Electronic Commerce Diretive Recital 46

[116] Decision of the *Tribunal de grande instance de Paris, Ordonnance de référé* of 22 June 2007, Jean Yves L. dit Lafesse v. Myspace, available at: http://www.legalis.net/jurisprudence-decision.php3?id_article=1965

structure with frames which is made available to its members" and significantly, "broadcast advertising upon each visit of the webpage form which it profits".[117]

However, the Electronic Commerce Directive exempts intermediaries for liability, granting them total immunity. Recital 42 of the Directive stipulates that the exemptions from liability established in the Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

In the US, Section 230 of the Communications Decency Act[118] provides immunity to blogs and social networking sites from liability resulting from the publication of information provided by third parties. If they create the content, they will not benefit from the protection of Section 230.[119] Section 512(c) of the Digital Millennium Copyright Act limits liability for copyright infringement from blogs and social networking sites that allow users to post content, if the website has a mechanism in place that allows copyright owners to request the removal of infringing content.

Regarding the liability under the Data Protection Directive, the activities of social networking websites such as the collection of users' data and their storage, would fall under the category of data processing operations, as defined in Article 2 of the Directive.

---

[117] Edwards in Edwards and Waelde (n 112) p.72
[118] 47 U.S.C. § 230: US Code
[119] *Doe v. MySpace, Inc.,* 474 F.Supp.2d 843, 845-846 (W.D. Tex. 2007)

8 The Challenges for the Protection of Personal Data in the European Union - The Commissions Consultation

As previously noted, in November 2010 the European Commission published a Consultation on the Commission's Comprehensive Approach on Personal Data Protection in the European Union[120] with the goal to obtain different opinions on how to address the new challenges for personal data protection in the Union.

One of the key objectives of the Commissions' Comprehensive Approach on Data Protection which concerns the social networking websites as well is enhancing control over one's own data. Users should always be able to access, rectify, delete or block their data, unless there are legitimate reasons, provided by law, for preventing this. Social networking websites to a great extent challenge the user's effective control over his or her personal data because they cannot always retrieve their personal data, like pictures for example, and are impeded in exercising their rights of access, rectification and deletion.[121] A possible solution could be the "right to be forgotten" - the right to withdraw consent to data processing, as proposed by the Commission.[122]

In recently published response to the Commission's Public Consultation (January 2011) the European Social Networks proposed to incorporate the principle of data processing for the user with respect to the issue of control of data, taking into account the way users initiate the processing of personal data in online social networks. [123] In their view further clarification is necessary of the lawfulness of transferring data on behalf of the user. This is the situation when the transmission of personal data is initiated by the user of a social network and the social network as data controller is processing these data of the user that include friends' data as well. Here, it is the end user that initiates and benefits from this procession of data.

---

[120] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4th November 2010

[121] Ibid. p. 8

[122] Reding, Viviane, Vice-President of the European Commission, EU Justice Commissioner "Your Data Your Rights: Safeguarding Your Privacy in a Connected World" Speech 11/183, Brussels, 2011

[123] European Social Networks Response to the Commission's Public Consultation on the Comprehensive Approach on Personal Data Protection in the European Union, European Social Networks, c/o Xing AG, Gaensemarkt 43, 20354 Hamburg, Germany, ID number: 19984124971-53 (Representing 9 European social networks with more than 60 million registered users), January 2011, p.3 <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/europeansocialnetworks_en.pdf>

With respect to the right to be forgotten**,** the European Social Networks are not in favor of imposing a mandatory date of expiration because of the technical possibilities of storing and copying data. According to them, users always have the possibility of deleting their personal data or leaving the network and thereby being deleted from the system. Also, they are against introduction of a mandatory data portability clause applicable to the social networking.

According to ETNO, the right to be forgotten is not a new concept and can be found in the current Directive. The basic principles such as Data Quality (art. 6), Right of access and Right of rectification (art. 12) and Consent (art. 7) ensure what is now referred to as the new "right to be forgotten".

One of the questions raised under the key objective of enhancing the internal market dimension and related with the social networking websites was how to revise and clarify the existing provisions on applicable law in order to improve legal certainty. This question emerged as a consequence of the fact that rising technological developments provide a possibility for data controllers established outside the EU to offer services from a distance and to process personal data of the EU citizens. Many internet players based outside the EU base their business model on on-line customer profiling and behavioral advertising, leveraging a lighter application of the privacy protection regime.[124]

In the view of the Commission, data subjects in the Union should be provided with same level of protection, regardless of where the data controller is geographically located and where the equipment used for the processing is located as well.

"The Commission considers that the fact that the processing of personal data is carried out by a data controller established in a third country should not deprive individuals of the protection to which they are entitled under the EU Charter of Fundamental Rights and EU data protection legislation"[125]

Viviane Reding, the EU Justice Commissioner, in a speech held on a Conference in London 2011 stated that the reform will encompass the principle of "protection regardless of data location" meaning that homogeneous privacy standards for European citizens should apply independently of the area of the world in which their data is being

---

[124] European Telecommunications Network Operators Association (ETNO) Reflection document on the EC Public Consultation on the Communication of a Comprehensive Approach on Personal Data Protection in the European Union <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/etno_en.pdf>

[125] Communication from the Commission (n 120), p. 11

processed and regardless of the geographical location of the service provider and the technical means used to provide the service. She pointed out that there should be no exceptions for third countries' service providers controlling European citizens' data and all companies operating in the EU market or any online product that is targeted at EU consumers must comply with EU rules.[126]

For example, a US-based social network company that has millions of active users in Europe needs to comply with EU rules. To enforce the EU law, national privacy watchdogs shall be endowed with powers to investigate and engage in legal proceedings against non-EU data controllers whose services target EU consumers.[127]

The European Social Networks in their response argued that in order to strengthen the sustainability of the Directive, it is necessary to ensure that the Directive applies to both European and non-European providers whose online services explicitly target European consumers.[128] According to them, EU Data Protection Law should be applicable to any online product that is targeted at European consumers regardless of the technical means used by a non-European provider. The current lack of control over non-European entities without permanent physical presence in the EU creates competitive disadvantage for European providers in the international online market.

In accordance with Article 6 of Rome I[129] the Data Protection Law should also be applicable if an online product is targeted at European consumers. The same applies if other criteria (e.g. national domain like „de.-domain", content, language) show that the processing of personal data of European individuals is intended.

The same point of view is expressed by Privacy International, privacy advocacy group, in their response to the Commissions' communication. Namely, if services are targeted at EU citizens, the law of the data subject country of residence should apply.

Similar view to the one of the European Social Networks and Privacy International has the European Telecommunications Network Operators Association (ETNO). In its Reflection document on the EC Public Consultation on the Communication of a Comprehensive Approach on Personal Data Protection the Association points out that with

---

[126] Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner Assuring data protection in the age of the internet British Bankers' Association Data Protection and Privacy Conference London, June 2011

[127] Reding (n 122)

[128] European Social Networks Response to the Commission's Public Consultation (n 123)

[129] Regulation No 593/2008 of the European Parliament and of the Council of 17th June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L117/6

regard to the applicable law when the data controller is not established on EU territory, the current criteria of use of equipment situated within the EU (Article 4 of the Directive) should be substituted and the criteria of "services targeting EU citizens" should prevail.[130] In addition, a level playing field should be granted for all subjects operating websites and services which target European citizens, regardless of the fact that the controller has an establishment within the EU.

Facebook response to the consultation was that improved legal certainty in the area of applicable law would be helpful and should recognize the developments of modern internet services such as Facebook. If such innovative businesses are to be able to develop, then the requirements for them to understand and comply with data protection law across multiple jurisdictions should not exceed their capacity to meet them.[131]

The Article 29 WG Opinion 8/2010 on Applicable Law refers to the need to consider additional criteria, in cases when the controller is established outside the EU but it is targeting EU individuals.

Of the proposed amendments of significance for the social networking websites, in my opinion users should have the right to be forgotten and be able to delete permanently all the information collected about them. With regard to the issue of applicable law I support the view that the targeting test should be applied, namely the Directive should apply to both European and non-European providers whose online services explicitly target European consumers, even though in many cases there might be difficulties to determine when an online activity is targeted at a particular State.

This line of reasoning can be seen as well in the Lindquist case. In its decision in this case the European Court of Justice found that the Directive's rules on international data transfers should not be applied to activities that could result in EU data protection law being applied indiscriminately to the entire Internet. Applied analogously, the Court's reasoning suggests that application of EU data protection law under Article 4 should be limited to cases in which the non-EU data controller has taken some action to target individuals in the EU.[132]

---

[130] European Telecommunications Network Operators Association (n 124)
[131] Facebook Response to European Commission Communication on personal data protection in the European Union prepared by representatives of Facebook Ireland Ltd. and Facebook Inc. http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/facebook_en.pdf
[132] C Kuner (2010) Data Protection Law and International Jurisdiction on the Internet (Part II) *International Journal of Law and Information Technology*, 1-21, p.14

The final decision of the European Commission on these issues is still pending, the reform package has still not been revealed to the public.

9 Conclusion

With the expansion of the internet in the last decade the social networking websites became inevitable part of our everyday life. The concerns about breaches of individuals' privacy and data security became more prominent as well, as a consequence of the very nature and functioning of the social networking sites. Even though people claim to be very concerned about what information about them are publicly revealed, this seems not to be true in the social networking world. People are prone to reveal much more about them online, if asked or just by own will, then in the real life world, if stopped on a street for example. Therefore, in order to protect users' privacy and reduce the risk of unlawful processing of users data by third parties the default settings of the social networking websites should be privacy-friendly and should give users the possibility to consent to any access to their profile's content that is beyond their list of contacts. Thus opt-in, instead of opt-out procedures should be applied by the social networking sites.

Considering the relevant provision of the Data Protection Directive, data controllers with respect to the social networking services will be the social network providers, as they determine the means for the processing of users' data and the purposes and management of the users' accounts such as the account registration and deletion. Application providers are also data controllers.

Having in consideration the fact that the definition of data controller is very broad, encompassing any natural person who determines the purposes of processing personal data, not only the social networking sites but also their users, individuals who post information about them and their friends might be regarded as data controllers as well.

The applicability of the EU Data Protection Directive to social networking sites which headquarters are located in third countries outside the EU is important in the cases of an alleged breach of the EU users' data protection rights by these social networking websites. This is essential for Facebook users, as one of the major social networking site

with headquarters in US. It is vital to distinguish whether EU users can rely on their national data protection legislations in the case of privacy infringement.

With respect to the application of Article 4(a) on the case of Facebook two situations can be distinguished. In the first situation users are uploading their data on the Facebook website directly to US. In this case EU data protection laws cannot be applied to protect the data rights of EU residents, because they are voluntarily submitting their data outside the reach of EU jurisdiction.

The second situation would be the one where Facebook establishments in Europe are processing data in EU, in the context of their activities, which would have as a corollary Facebook being under the obligations arising from the European data protection laws based on the EU Data Protection Directive. However, information about the exact nature of the activities of the Facebook offices located in Europe and, most important, whether they are involved in data processing is very difficult to obtain.

Pursuant to Article 4(c) the national law of a member state would apply if the data controller is not established within the EU but uses equipment located on the EU territory for purposes of processing personal data.

If the Opinion 5/2009 on online social networking is followed, the provisions of the Data Protection Directive and respectively the national laws of all 27 EU Member States will apply to data processing operations of social networking sites such as Facebook.

Considering Article 4(1)(c) in this way gives rise to the possibility of regulatory overreaching in the online environment. In order to create level playing field the new amendments of the EU Data Protection Law should ensure that the applies to both European and non-European providers whose online services explicitly target European consumers. Namely, the targeting test should be applied.

The major concerns arising out of the increased popularity and utilization of the social networking sites is the potential threat to users' privacy.

A possible solution to the potential treat to the users privacy by application providers would be if the access of application providers to users' personal data is limited to only that information actually necessary for the functioning of the application, not unrestricted as it is, to collect all the data from a users' profile. Also, the manner and purposes for which they use these data should be under stricter control as well. The social networking site should exercise control over the amount of information collected by

the application providers and should develop some kind of technical means to limit the access to users' data.

Regarding the photo tagging, users should be asked for prior consent for storing their biometrical data and for the subsequent use of these data. Also, they should at least receive tag suggestions, and then have the possibility to accept or reject the tag suggestion.

Facebooks' practice of tracking users via the Like button infringes the data protection law principles. Data protection authorities should undertake necessary measures to protect users from this kind of infringments, as well as from the practice of keeping data disclosed on the sites for unlimited time.

The proposed solution would be the "right to be forgotten" - the right to withdraw user consent to data processing.

For the users point of view it is important to distinguish whether social networking sites should be regarded as a private space where the user has reasonable expectations of privacy or a public space. If they are to be treated as private space where the user has reasonable expectations of privacy, then the utilization of users' posts and photos as evidence in proceedings against him would arguably breach his privacy. Different would be the outcome if the social networking sites are treated as public space, where it will be questionable whether privacy would be protected.

With respect to the social networking sites responsibility as platform providers where users publish various types of information, they should be jointly responsible for the content published because they make profits and because they are aware that some of the content published is illegal.

9.1 References

List of Judgements/Decisions

Doe v. MySpace, Inc., 474 F.Supp.2d 843, 845-846 (W.D. Tex. 2007)

Katz v United States, 389 U.S. 347 (1967)

Lindqvist, C-101/01 [2004] 1 CMLR 20

Jean Yves L. dit Lafesse v. Myspace, Decision of the *Tribunal de grande instance de Paris, Ordonnance de référé* of 22 June 2007

Treaties/Statutes

Regulation No 593/2008 of the European Parliament and of the Council of 17th June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L117/6

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce) [2000] OJ L178/1.

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

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly a vailable electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4th November 2010

Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Paris, 1980)

Secondary Literature

Books

LA Bygrave LA, *'Data Protection Law: Approaching Its Rationale, Logic and Limits*' (Kluwer Law International, The Hague / London / New York 2002)

Bennett CJ, Raab C '*The Governance of Privacy: policy instruments in a global perspective'* (2nd Edition, MIT Press, London 2006)

Articles

Acquisti A, Gross R, (2006) 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook' Proceedings of 6th Workshop on Privacy Enhancing Technologies, Lecture Notes in Computer Science 4258, *Springer*

Alsenoy V, Ballet B, Joris et al. (2009) 'Social networks and web 2.0: are users also bound by data protection regulations?' available at <http://www.springerlink.com/content/u11161037506t68n/fulltext.pdf >, IDIS

Article 29 Data Protection Working Party: Opinion 1/2008 on Data Protection Issues Related to Search Engines (WP 148) (04.04.2008)

Article 29 Data Protection Working Party: Opinion 5/2009 on online social networking (WP 163) (June 12, 2009)

Bygrave LA, (2000) 'Determining Applicable Law pursuant to European Data Protection Legislation' *Computer Law & Security Report*

Boyd D, N Ellison, (2007) 'Social network sites: Definition, history, and scholarship' *Journal of Computer-Mediated Communication*, *13*(1), article 11

Edwards L, (2009) 'The Fall and Rise of Intermediary Liability Online' in L Edwards, C Waelde (ed) "*Law and the Internet*" (Third Edition, Oxford, Hart Publishing, 2009)

Edwards L, (2009) 'Privacy and Data Protection Online: The Laws Don't Work?' in L Edwards, C Waelde (ed) '*Law and the Internet'(* Third Edition, 2009, Hart Publishing)

Edwards L, Brown I, (2009) 'Data Control and Social Networking: Irreconcilable Ideas?' in A Matwyshyn (ed.) '*Harboring Data: Information Security, Law and the Corporation'* (Stanford University Press)

Garrie D, Wong R, (2010) 'Social networking: opening the floodgates to personal data' *Computer and Telecommunications Law Review*, 16(6)

Graham N, Anderson H, (2010) 'Are individuals waking up to the privacy implications of social networking sites?' *E.I.P.R.* 32(3)

Henson B, Reyns B and Fisher B, (2011) 'Security in the 21st Century: Examining the Link Between Online Social Network Activity, Privacy, and Interpersonal Victimization' *Criminal Justice Review*, 36(3)

Hodge M, (2006) 'The Fourth Amendment and privacy issues on the "new" Internet: Facebook.com and MySpace.com.' *Southern Illinois University Law Journal*, 31, 95-122

Kosta E, (2010) 'The Freddi Staurs of Social Networking – A Legal Approach' in M. Bezzi et al. (Eds.): *Privacy and Identity* (IFIP AICT 2010)

Kuner C, (2010) 'Data Protection Law and International Jurisdiction on the Internet (Part I)' *International Journal of Law and Information Technology* 18(2)

C Kuner (2010) Data Protection Law and International Jurisdiction on the Internet (Part II) *International Journal of Law and Information Technology*
Kuczerawy A, (2010) 'Applicable data protection law in a relationship between EU users and non-EU based Social Networking Site' in M. Bezzi et al. (Eds.): *Privacy and Identity* (IFIP AICT 2010)

Lawson P, (2008) 'Reply to the Canadian Privacy Commissioner regarding the PIPEDA Complaint: Facebook' Canadian Internet Policy and Public Interest Clinic

Moerel L, (2011) 'The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to processing of Personal Data of EU Citizens by Websites Worldwide?' *International Data Privacy Law,* 2011, 1(1)

Reding V, Vice-President of the European Commission, EU Justice Commissioner "Your Data Your Rights: Safeguarding Your Privacy in a Connected World" Speech 11/183, Brussels, 2011

Reding V, Vice-President of the European Commission, EU Justice Commissioner 'Assuring data protection in the age of the internet British Bankers' Association Data Protection and Privacy Conference London, June 2011 <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/452&format=HTML&aged=0&language=EN&guiLanguage=en>

Roosendaal A, (2010) 'Facebook Tracks and Traces Everyone: Like This!', Tilburg law School research paper, Electronic copy available at: <http://ssrn.com/abstract=1717563>

Wong R, (2008) Social Networking: Anybody is a Data Controller! Electronic copy available at: <http://ssrn.com/abstract=1271668>

Wong R, Savirimuthu J, (2008) 'All or nothing: this is the question?: The application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet' *John Marshall Journal of Computer & Information Law*, 25(2)

A