Facebook and its EU users - Applicability of the EU data protection law to US based SNS

Aleksandra Kuczerawy

Facebook and its EU users – Applicability of the EU data protection law to US based SNS*

Aleksandra Kuczerawy
Interdisciplinary Centre for Law & ICT (ICRI) – K.U.Leuven
Sint-Michielsstraat 6, 3000 Leuven, Belgium
aleksandra.kuczerawy@law.kuleuven.be

Abstract: The present paper examines the problem of applicable data protection law in a relationship between EU users and non-EU based Social Networking Site (SNS). The analysis will be conducted on the example of Facebook, which is one of the most popular SNS. The goal of the paper is to examine whether European users of Facebook can rely on their national data protection legislations in case of a privacy infringement by the SNS. The 95/46/EC Directive on Data Protection provides several options to protect EU residents in such relation. The paper will analyze whether Facebook's participation in the Safe Harbor Program means that it is a subject to the regulation of the Data Protection Directive. Then, the paper will discuss if data processing activities of Facebook fall under the scope of the Data Protection Directive at all.

Keywords: Social Networking Sites, data protection, applicable law, cookies, transfer of data to third countries

1 Introduction

Social Networking Sites (SNS) are a phenomenon of social interactions that became part of our lives faster than anybody could have imagined. Widely accessible platforms where people share data became very popular worldwide and have a constantly growing number of users. In Europe, many SNS have developed targeting the audience of the country where they are based. Each European country has a preferential SNS (Hyves in the Netherlands, StudiVZ in Germany, NetLog in Belgium or NaszaKlasa in Poland). Additionally, there is also a number of SNS originating from the USA that have users throughout the whole of Europe. Whereas the European based SNS are without any doubt subject to their national privacy laws, the situation of US based SNS is not that clear. Insofar as US based SNS are providing a service from the US, although directed to users worldwide, the applicability of the European privacy regime as defined by the Data Protection Directive (hereinafter DPD or the Directive)[1], is being debated. The apparent similarity of EU based and US based websites, which provide the service in the native language of the user, could mislead their users and make them believe they could enjoy the same level of protection. It is thus crucial to define the situation of such foreign based SNS regarding the applicable data protection law when dealing with European users. In order to find an answer to the complex issue of applicable law this article will rely on the example of Facebook as one of the most popular SNS in both the USA and Europe.

The problem of determining the applicable law for online interactions is not a new one. With the advent of the Internet it became immediately clear that one of its main characteristics is a lack of territorial borders. In a traditional setting, the national borders help to indicate an appropriate national law to be applied. With the absence of that factor alternative solutions had to be found to adjust to the new situation. Concerns have risen in particular in Business to Business (B2B) and Business to Consumer (B2C) online contracting with regard to the applicable contract law and consumer law. The question is now being raised for the applicability of data protection laws.

First concerns have emerged with regard to the applicability of the EU regime to data processing activities of search engines. The Article 29 Working Party[1] in this case stated that the EU data protection law applies if a non EU based search engine makes use of cookies on the territory of the EU. The question however pops up again with regard to SNS as they are called to process a large amount of personal data of their users. But can the same solution, as the one used for search engines, be relied on when it comes to SNS? This article will discuss such possibility analysing the specific situation of the US based SNS Facebook because of its popularity among European users. It will first highlight Facebook's participation in the Safe Harbor program. The article will focus on the very specific issue of the applicability of data protection law for EU users of a non-EU based Social Network. It will exclusively focus on the relation between the SNS providers and its users, not entering into other concerns that could arise with regard to the applicable regime to relations between users of SNS[2].

2 Situation of Facebook

Facebook is a non-EU based social networking site. Its main place of establishment is Palo Alto in California, USA which makes it a subject to the US law [3]. Facebook offers its services all over the world, and a substantial proportion of its users are based in the EU.

First of all, it should be clarified that the services offered by Facebook as a SNS provider constitute 'data processing' in the light of the DPD. '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,

* Part of the research leading to these results has received funding from the European Community's Seventh Framework Program (FP7/2007-2013) under grant agreement n° 216483. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

1 Under Article 29 of the Data Protection Directive, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data is established, made up of the Data Protection Commissioners from the Member States together with a representative of the European Commission. The Working Party is independent and acts as an advisory body. The Working Party seeks to harmonize the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection issues.

2 For the applicability of the Data Protection Directive to users of SNS see [2].

alignment or combination, blocking, erasure or destruction [1]. As the definition is very broad, it undoubtedly covers activities performed by providers of SNS who, at least, collect and store data of their users.
Furthermore, Facebook is in the position of data controller, as an entity which alone or jointly with others determines the purposes and means of the processing of personal data [1]. As expressed in several opinions, by providing the technical side of the service, in other words by making it possible to actually process data on the website, the provider determines the purposes and means of the data processing [4]. Due to these circumstances, Facebook can be described as a US based data controller involved in the processing of personal data of European individuals.

3. First hope: Facebook as a member of Safe Harbor

3.1 Safe Harbor program

When looking at Facebook's privacy policy [5], one can see that the company is a member of the EU Safe Harbor Privacy Framework [6]. The Safe Harbor program was developed by the US Department of Commerce in consultation with the European Commission. It was introduced to solve the problem created by the new regime regulating transfers of personal data established by the Directive. Such transfers are prohibited whenever the country where the data is imported does not guarantee an adequate level of protection – like the USA where the data protection is based on self-regulatory approach.
The Directive provides a series of derogations to the prohibition of transfers of data to third countries if adequate safeguards of protection are guaranteed, e.g. through contractual agreements [7]. Such possibility has been introduced in art. 25.6 of the Directive. The Safe Harbor renders data transfers possible on condition that companies importing personal data commit themselves to a set of privacy principles negotiated by the US Department of Commerce and the Commission. Such commitment is established through a voluntary subscription to the Safe Harbor program.
The Department of Commerce provides a list of requirements that have to be fulfilled by the company in order to be able to join. The list of necessary steps consists of: company's self-assessment whether it is eligible for participation in the program; determination of dispute resolution and enforcement mechanisms; submission of a written certificate to the Department of Commerce; disclosure of the company's commitment to the Safe Harbor principles; implementation of the Safe Harbor principles in practice; and reaffirmation of the membership on annual basis [8]. Companies that are eligible to participate in the program are those that are subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of the Transportation (DOT). Once a company fulfils these criteria it is signed up to the program. It is not however within the scope of competence of the Department of Commerce to examine a company's situation with regard to the EU data protection law as long as such companies remain subject to US law for the processing of personal data on US territory.
As a consequence of a subscription, data collected in the EU can be transferred to the US for further processing. Once in the US, the data are deemed to be protected under principles similar to those of the DPD [9]. For the European data

subject this means, apart from the guarantee of the adequate protection, that any claims brought by the European residents against US companies will be heard in the US, in accordance to the US law [10].

3.2 Transfer or not?

Undoubtedly, it was very cautious of Facebook to subscribe to such program. However, was it necessary? From a legal perspective, only if Facebook is being transferred personal data collected in the EU, would it need to join the program.

First of all, it should be noted that provisions of art. 25 DPD are addressed to the controller based in the EU. The concept of data transfer to third countries refers to the situation when there is a data controller on the territory of the EU who collects the data of the EU individuals and exports them to another controller (or a processor) outside of the EU. It means that two different actors are necessary to participate, both of them acting as separate data controllers or as a controller and a processor[3]. Moreover, in case the data transfer occurs, there is an obligation of compliance with the law of the location in which the data is collected, before it is sent outside of the EU [11]. It is normally a responsibility of the data exporter, i.e. the controller in the EU. It would imply that an entity collecting data for Facebook in the EU, such as a local branch of the company, is under such obligation.

According to the information provided on the website of Facebook, its headquarters are based exclusively in the US. When feeding Facebook with their data, users are thus sending them directly to the US. There is no EU-based intermediary in the processing of these data. We should then consider, in such case, that there is a lack of one (transferring) party because the US company does not act as an EU controller. Therefore, it is not really a transfer of data in the understanding of the Directive [12]. In absence of EU based controller, the provisions of article 25 and 26 DPD, do not apply to this situation. For that reason, the US company does not need to comply with the restrictions for data transfers [11].

It is thus surprising that Facebook has opted for subscribing to the Safe Harbor program. In practice, even though the 'real' transfer does not occur, the US Department of Commerce accepts Safe Harbor subscriptions from US based companies that only process the personal data of European users from their US websites [11].

Facebook was of course free to do so, as the Safe Harbor is a voluntary program. However, such decision does not mean that it committed to comply with the EU Data Protection law. It only means that it committed to a US voluntary program improving the level of protection of their users' data with regards to the protection as provided in the US.

As shown above, as long as the user sends his data directly to the US without any intermediary in Europe, the regime of international transfers of personal data cannot

---

3 'Data controller' means the 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 (art. 2(d)DPD). 'Data processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (art. 2 (e)DPD).

apply. This leads to a more fundamental question whether the processing of European users' data by a US based SNS could fall under the provisions of the EU Directive. To that effect, it is necessary to determine whether art. 4 of the DPD, which defines the rule of choice of law, applies.
An important hint regarding the relation between art. 4 DPD and art. 25 DPD was given by Art. 29 WP. In its Opinion about the level of protection provided by the Safe Harbor it stated that the program does not affect the application of Article 4 of the Directive [13]. This means that the Principles of Safe Harbor were not intended to substitute the national provisions implementing the Directive in situations where those national provisions apply. The following section will hence analyse the applicability of the national data protection regulations.

4 The specific rule of choice of law of art. 4: towards a solution?

Art. 4 of the Data Protection Directive addresses the problem of applicability of national data protection laws of the Member States. Despite the complexity of the issue, due to its international character, art. 4 has not been extensively analyzed so far [14]. This is quite remarkable, considering the possible broad impact of the provision.
Art. 4 prescribes the application of the national data protection laws of the EU Member States when a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of that Member State, when b) the processing is carried out on the territory where the law of a Member State applies, and c) when the controller is located outside of the EU but it uses equipment on the territory of a Member State. Art. 4.1(a) could apply if European offices of Facebook were involved in processing of the European users' data. However, information about the exact nature of the activities of the offices located in Europe and, most important, whether they are involved in data processing is very difficult to obtain[4]. For this reason the analysis will focus on the 'equipment criterion' of art. 4.1 (c).

4.1 Use of equipment

Article 4.1(c) of the DPD states that each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where 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 [1]. This means that EU countries can directly apply their national data protection legislations to non-EU based websites whenever they would make use of equipment located on the territory of the said countries (but not when the equipment is used solely for the transit purposes).
Does this apply to Facebook then? Here, it is necessary to enter into a discussion about the interpretation of the term 'equipment'. According to the Art. 29 Working Party it is a decisive factor for the application of the European data protection law. Such 'equipment' should be at the disposal of the controller for

[4] Questions sent to Facebook through the Privacy Help Center were left unanswered.

the processing of personal data [15]. However, it does not have to be a full control but it is sufficient that the controller determines which data are collected, stored, transferred, altered etc., in which way and for which purpose [15].
It is a strong opinion of the Art. 29 Working Party that the user's PC constitute exactly the type of equipment described in the working document [15]. To apply this criterion, it is sufficient for the controller to make use of the users' PC by placing cookies on the hard disk. The national law of Member State where the user's personal computer is located would then apply to the question under what conditions user's personal data may be collected by placing cookies on his hard disk [15]. Such is the case of Facebook [5]. It follows that Facebook users' national law of EU Member State would be applicable to the processing.
This position has been confirmed by the Art. 29 WP opinion on search engines [16], and a recent opinion on online social networking [17]. Such an approach, however, might have very severe effects. It could lead in fact to a direct application of the Directive, and consequently of the national data protection laws of all EU countries to every non-EU based website using cookies with users on the territory of the EU [18]. So basically, it could apply to the entire Internet [11]. On the one hand, it seems to shield European users in case of any processing of their data as it puts them under the full protection of the European data protection law. Such an extent of protection would be satisfying and definitely enough, from the DPD point of view, to protect the privacy of European residents. Hence, it could end the discussion at this point. On the other hand, it makes the situation of all non-EU based data controllers involved in the processing of data of European users extremely complicated. When applying such interpretation to the analyzed case, the result would be that Facebook has to simultaneously comply with data protection legislations of each EU country where the users enjoy the service (so practically all 27 Member States). Such requirement is in many views not pragmatic. Moreover, it is described by some authors as an 'impossible burden' [11].
Here it should be mentioned that in the traditional, off-line setting any company doing business in another country has to do so in compliance with the local law, and there is nothing unusual about it. Moreover, it refers to all areas of law, including data protection law. Sometimes the need of compliance is even taken to a higher level when the weaker party is given a special amount of protection. A perfect example of such regulation is consumer law. It provides the protection of the local law of the consumer irrespectively of the location of the seller [19]. Moreover, this principle cannot be ruled out through a choice of law clause in the contract. Maybe it would be worth considering whether data subjects, who undoubtedly are the weaker party, should not be granted protection embedded in the similar idea. However interesting the question is, it is beyond the scope of this article. But it shows that the requirement of compliance with the local law of the user is not an extravagant concept. So is the situation of Facebook so much different to see such a requirement as an impossible burden?
Currently, the broad scope of application of art. 4.1 c DPD is a result of the Art. 29 WP's interpretation of the term 'equipment' and not of the wording of the Directive. This broad effect seems to be going further then originally designed

back in 1995 when the use of technologies like cookies was not so common[5]. These are the reasons why this provision causes heated discussions and is often criticized. Defining such a broad scope of art. 4.1.c in the Directive itself would undoubtedly provide stronger legal basis to effectively protect EU data subjects in relations with non-EU data controllers. This is definitely one of the issues that could be clarified during the next revision of the Directive.

4.2 Limits of the "cookies" solution

In many ways the "cookies" criterion appears insufficient to provide a satisfying answer to the problem at stake. The artificial nature of such construction is even more striking when we look into the E-privacy Directive [21]. The former wording of the article 5.3 of the 2002 E-privacy Directive prescribed that the use of cookies should be only allowed when the user is informed about it, in a clear and comprehensive way, in accordance with the DPD, and is offered the right to object to such processing by the data controller [21]. The recent amendments to the Telecoms package, introduced at the end of 2009, modified the wording of this provision and now it requires the user's prior consent before the installation of cookies on his computer [22]. This change has attracted lot of attention from the industry but it is still unclear how will it influence the discussed problem.

The user must be notified when the cookie is installed on his computer. If he doesn't agree to that, a paradoxical situation could occur. 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. This would happen because art. 4.1 (c) DPD applies only if the data controller uses equipment, so the user's computer, on the territory of the Member State, through the cookie. This situation would however not occur in case of user's objection to the use of cookie. Thus, there would be no ground to apply art. 4.1 (c) DPD.

The whole situation is spiced up by the fact that most of the time the user refuses the cookie in a belief that he is protecting his own privacy. However, many services are not possible to enjoy without accepting the cookies, and Facebook is no exception here. It is undeniable that the problem of the protection of the collected data would disappear if the service could not be provided without the use of cookies. In the former version of the Facebook 's Privacy Policy, users were informed that "[they could] remove or block this [persistent] cookie using the settings in [their] browser if [they] want[ed] to disable this convenience feature". In the new Privacy Policy, in life since November 2009, users are however informed that opting for the removal or blocking of cookies "may impact [their] ability to use Facebook"[5]. Therefore it seems not possible to enjoy the full service without having previously accepted the use of cookies. Although this seems to simplify the problem of the privacy protection, it however raises questions about a real possibility of users to object to the use of cookies in practice.

The arguments above create an inevitable impression that 'the cookie construction' from art. 4.1(c), although designed to provide a basis for the protection of the European residents' data, is in fact an artificial rule that may be too weak to

[5] Cookies technology was developed in 1994, see more in [20].

provide an efficient protection in practice. Such a conclusion can be drawn especially in light of the obligation installed by art. 5.3 of the E-privacy Directive to require users' consent for the use of cookies. The shield provided by art. 4.1 (c) DPD can be easily removed by the user acting in a good faith. An inevitable impression is created that cookie construction does not provide a workable solution and, in fact, when put into practice can lead to more questions than answers. For this reason it can only be considered as a temporary solution which should be reconsidered with the next revision of the Data Protection Directive.

4.3 An illusory protection

Another aspect of the problem is related to the most often heard criticism of art. 4.1(c): the difficult enforceability of the provision. The assumed power of an EU Member State to apply its national data protection legislation to a non-EU website processing data of its citizens by means of cookies is not synonymous with that Member State's ability to enforce such judgment [11].

The Article 29 WP was fully aware of that difference. For that reason, it called for caution in applying art. 4.1(c) to concrete cases. The objective of the rule is to ensure that individuals receive protection of their national data protection laws in those cases where it is necessary, where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved [15]. At the same time, the Working Party believes that many third countries will recognize and enforce such judgment [15]. Moreover, it presents an opinion that in third countries where data protection rules and authorities are in place, enforcement will not be a problem [15]. This however is not a common opinion. According to Kuner, enforcement in this case seems very unlikely. In his view, every unsuccessful attempt of enforcement would only lead to undermining of the general respect for data protection law [11]. He also recalls the even stronger opinion of Mann who calls a similar attempt a violation of international law [11]. It is considered that an idea of any State trying to enforce its own law on foreign actors outside its borders is simply against commonsense and the present international order [23].

Given these arguments, an additional observation can be made. It has to be emphasized that applicable law, jurisdiction and enforcement are three related, but separate questions. For each one of them there are specific rules. Therefore, the weak chance of enforcement should in general not be a reason to disregard a correctly determined applicable law.

5 Conclusion

The situation of the European users of Facebook, regarding the issue of the applicable data protection law is neither clear nor easy to solve.

First unclarity stems from Facebook's participation in the Safe Harbor program. A lack of controller in Europe, participating in the process, point to the fact that there is no transfer of data. It means that there is no addressee of art. 25 DPD and the special restrictions for data transfers to third countries do not apply to the situation under discussion. The fact that Facebook has decided to join the Safe Harbor program is in any case beneficial for EU users as it improves the level of protection of their data in the US. However, as shown in this article, this

does not mean that Facebook complies with the DPD. Additionally, it could mislead its users with regards to the real level of protection ensured.

In order to determine whether Data Protection Directive is applicable one should look into art. 4.1(c) which is directed to the non-EU based data controllers who use equipment in the EU. The Art. 29 WP has recently clearly stated that the provisions of the Data Protection Directive apply to SNS providers in most cases, even if their headquarters are located outside of the EEA [17]. It reached this conclusion by acknowledging 'cookies' as a way of making use of equipment (in the form of user's computer) on the territory of the Member States. So, it seems that the processing of users' data would be regulated directly by the European data protection law, and consequently by the user's national law.

This approach, however, is heavily criticized, for several reasons. One of them refers to weak chances of enforcement of a decision taken on the basis of this rule. Moreover, an obligation to comply with the national data protection laws of the EU countries, because of use of cookies, is often considered as a burden too heavy for the providers of services from outside of the EU. Furthermore, there is a risk that for any service allowing its users to enjoy it with disabled cookies, the protection spread over the EU individuals with the 'cookie provision' could be easily eliminated by the users themselves, in an attempt to protect their privacy. All these critical arguments, thus, create an impression that art. 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 SNS.

It can be clearly concluded that the current situation provides no legal certainty. It undoubtedly calls either for another solution, or for a stronger legal basis for the existing one. Unfortunately, until now there is no case law that would help to find criteria of interpretation.

The Art. 29 WP, in order to make the situation clearer, could maybe enter into discussions on this specific problem with Facebook. Such idea is based on the precedent of the discussions initiated with Google. In 2008 an attempt to address and seek industry perspectives on data protection issues related to search engines was made through an invitation to an open discussion placed in the Opinion 148. The 'call for opinion' was answered by Google which replied through an official 'Response to the Article 29 Working Party Opinion on Search Engines' [24] published on its website. In this document Google addressed problematic issues of data protection related to search engines and presented its point of view on the subject. The reply was undeniably a contribution to the discussion which could be repeated now.

Another example of openly addressing a service provider is a recent action of the Canadian Data Protection Authority which issued a report criticizing some points of Facebook's Privacy Policy and pointing out that such policy was not compliant with the Canadian Data Protection Law [25]. Quite surprisingly to most observers Facebook replied almost immediately organizing a set of meetings and promising to fix the controversial points which have not been solved immediately [26]. It will of course take some time to see how serious the promise was, however, the first step has been made and the dialogue has been started. What is the most important aspect here is the fact that the action of the Canadian DPA was not ignored by Facebook. In these circumstances maybe it is time for the Art. 29 WP to follow the

Canadian example in taking more dynamic steps and more actively target Facebook, as the US based SNS with the biggest number of users in Europe. There are more issues than only applicable law that could be discussed and hopefully solved that way.[6]

Acknowledgments. The author would like to thank Brendan Van Alsenoy, Fanny Coudert, Eleni Kosta and Karel Wouters for their support with legal and technical knowledge and their critical review of the solutions proposed.

References

1. Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), (OJ L 281, 23.11.1995)
2. Van Alsenoy B., Ballet J., Kuczerawy A., Dumortier J. 'Social networks and web 2.0: are users also bound by data protection regulations?', in: Identity in the Information Society (IDIS), 2009, Special issue on Social Web and Identity, DOI 10.1007/s12394-009-0017-3, available at: http://www.springerlink.com/content/u11161037506t68n/
3. Facebook Factsheet: http://www.facebook.com/press/info.php?factsheet
4. Wong R., Savirimuthu J., All or nothing: this is the question?: The Application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet
5. Facebook Privacy Policy: http://www.facebook.com/policy.php?ref=pf
6. Safe Harbor list of companies: http://web.ita.doc.gov/safeharbor/SHList.nsf/f6cff20f4d3b8a3185256966006f7cde/1c51b941879c2e87852572d700734dc1?OpenDocument&Highlight=2,Facebook
7. Safe Harbor, U.S. Department of Commerce, http://www.export.gov/safeharbor/index.asp
8. Helpful Hints Prior to Self-Certifying to the Safe Harbor: http://www.export.gov/safeharbor/eu/eg_main_018495.asp
9. Safe Harbor Principles and FAQ: http://www.export.gov/safeharbor/SH_Overview.asp; http://www.export.gov/safeharbor/SH_FAQ8.asp
10. Safe Harbor, U.S. Department of Commerce: http://www.export.gov/safeharbor/eg_main_018236.asp
11. Kuner C., European data protection law: corporate compliance and regulation, 2nd ed., New York, 2007
12. De Terwangne C., Louveaux S., Data Protection and Online networks, Computer Law and Security Report, vol. 13 no. 4 1997, pp. 234-246
13. Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles", WP 32 adopted on 16 May 200, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp32en.pdf
14. Perez Asinari Maria Veronica, International aspects of personal data protection *Quo vadis* EU? In: Challenges of privacy and data protection law, Perez Asinari Maria Veronica, Palazzi Pablo (eds.), Bruxelles, 2008, pp. 383-413

6 In the Report Canadian DPA addressed the following issues: collection of date of birth, default privacy settings, Facebook advertising, Third-Party applications, new uses of Personal Information, collection of Personal Information from sources other than Facebook, account deactivation and deletion, accounts of deceased users, Personal Information of Non-Users, Facebook Mobile and Safeguards, monitoring for anomalous activity, deception and misrepresentation.

15. Art. 29 Data Protection Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, WP 56, adopted on 30 May 2002
16. Art. 29 Data Protection Working Party, Opinion 1/2008 on data protection issues related to search engines, WP 148, adopted on 4 April 2008
17. Art. 29 Data Protection Working Party, Opinion 5/2009 on online social networking, WP 163, adopted on 12 June 2009
18. Terstegge J., in: Bullesbach A., Poullet Y., Prins C. (eds.), Concise European IT Law, Alphen aan den Rijn, 2005
19. Art. 12 of the Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (OJ L 144, 4.6.1997)
20. Schwartz J., 'Giving Web a Memory Cost Its Users Privacy' (4 September 2001) New York Times. at Al.
21. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive), (OJ L 201, 31.7.2002)
22. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, (OJ L 337, 18.12.2009)
23. F A Mann, The Doctrine of Jurisdiction in International Law, 1964, 111 Recueil des Cours 9, 145-146, as in: Kuner C., European data protection law: corporate compliance and regulation, 2nd ed., New York, 2007
24. Google's 'Response to the Article 29 Working Party Opinion on Search Engines': http://blogs.taz.de/ctrl/files/2008/09/google.pdf
25. Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC)
against Facebook Inc. Under the *Personal Information Protection and Electronic Documents Act* http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm
26. Facebook Announces Privacy Improvements in Response to Recommendations by Canadian Privacy Commissioner:
http://www.facebook.com/press/releases.php?p=118816