Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2009 Proceedings | Mediterranean Conference on Information Systems (MCIS)

2009

Facebook: Reconstructing Communication And Decostructing Privacy Law?

Anna-Maria Piskopani
University of Athens, piskopania@yahoo.gr

Lilian Mitrou
University of the Aegean, L.MITROU@AEGEAN.GR

Follow this and additional works at: http://aisel.aisnet.org/mcis2009

Recommended Citation
Piskopani, Anna-Maria and Mitrou, Lilian, "Facebook: Reconstructing Communication And Decostructing Privacy Law?" (2009). *MCIS 2009 Proceedings*. 70.
http://aisel.aisnet.org/mcis2009/70

This material is brought to you by the Mediterranean Conference on Information Systems (MCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in MCIS 2009 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

FACEBOOK: RECONSTRUCTING COMMUNICATION AND DECOSTRUCTING PRIVACY LAW?

Piskopani, Anna-Maria, University of Athens, Athens, Greece, piskopania@yahoo.gr
Mitrou, Lilian, University of the Aegean, 83200, Samos, Greece, L.Mitrou@aegean.gr

Abstract

The exponential growth of Facebook during the last year, was followed by a vital public discourse and often an alert with regard to the impacts of this popular SNS on communicational and behavioural attitudes and users' rights. In this Paper we focus on privacy issues relating to Facebook. We attempt to define the "phenomenon Facebook" as a social and communicational ecosystem in the context of Web 2.0. In this perspective we discuss the trust relationships evolved in the Facebook communities to the extent that they affect the perceptions and expectations of privacy. We refer to the privacy issues, focusing on shortcomings of the Facebook privacy policy and practices, on regulatory responses and the problems relating to consent and contract as privacy gatekeepers in SNSs. Finally, we try to identify how SNSs and Facebook pose new challenges to privacy and data protection law.

Keywords: *Facebook, Social networking sites, informational privacy law, data protection*

1 INTRODUCTION

Although Social Networking Sites [hereafter SNS(s)] existed for over a decade, it was the unprecedented success of Facebook, which has rendered them to a global trend. Facebook shares the characteristics of a "typical" SNS: it is an online communication platform, which enables individuals to construct a public or semi-public profile within a bounded system, in order a) to articulate a list of other users with whom they share a connection, and b) to view and traverse their list of connections and those made by others within the system (Boyd & Ellison's 2007). "Social networking' is enabled through the use of tools that provide a list of contacts for each user, and with which users can interact. An SNS provides also tools that allow users to post their own material, such as a photograph or a diary entry (Art.29 Working Party 2009).

The exponential growth of Facebook users, reaching in some countries an increase of 2900% (Italy) during the last year, was followed by a vital public discourse - and often an alert - with regard to the impacts of this popular SNS on communicational and behavioural features, on the structure of social relationships and –last but not least – on rights and liberties. Scholars have pointed out many legal aspects of the phenomenon: i.e. relating to copyright law (Hetcher 2008), right of publicity (Morganstern 2008), freedom of speech of minors (DiPietro 2008), political discourse (Kushin &Kitchener 2009), facial recognition (Polar 2007) etc. Press reports, privacy advocates, Data Protection Authorities (Art.29 Working Party 2009) and organizations (ENISA 2007) underlined the privacy risks and concerns deriving from the "participation" to the Facebook.

Is Facebook a new community, built by users, a new ecosystem or a new Cyber-Panopticon, where users offer the means for a total surveillance? Privacy concerns rely, among others, on the specific characteristics of Facebook: Its function, its worth lies exactly in the fact that the vast majority of users communicate using their real identity, providing their names and details of their life. The essential part of being in Facebook is to use your real name, so that people will search for you and add you to "their friends list". In our ongoing research, laid down briefly in this paper, we focus on privacy issues relating to Facebook. We attempt to define the "phenomenon Facebook" as a social and communicational ecosystem in the context of Web 2.0. In this perspective we discuss the trust relationships evolved in the Facebook communities to the extent that they affect the perceptions and expectations of privacy. We refer to the privacy issues, focusing on shortcomings of the Facebook privacy policy and practices, on regulatory responses and the problems relating to consent

and contract as privacy gatekeepers in SNSs. Finally, we try to identify how SNSs and Facebook pose new challenges to privacy and data protection law.

2 THE FACEBOOK PHENOMENON

2.1 A vivid ecosystem of Web 2.0 and/or a social "utility" ?

Facebook may be seen as informal but all-embracing identity management tool, defining access to user-created content via social relationships. Facebook builds in the new environment of Web 2.0., which is dominated "by user –generated content", by information produced, received, disseminated by "non-professionals", in particular, but non only, through SNSs. The paradigm of Internet changes: from static, isolated repositories of information is shifting to dynamic, user-driven and participatory sites. Facebook creators tend to define and present it as a "social utility". The term reflects website's function as an every day tool for the million of users, and also reveals Facebook's desire to become a utility, like a global service company, in which potentially billions of people use it in their personal and professional lives. Since 2007 Facebook makers set the goal that Facebook would become a pervasive ecosystem, really efficient for people to communicate, get and share information (Hansell 2008). That was an effectual strategy that led Facebook to have almost 200 million users worlwide and constantly expanding.

2.2 From advanced blog to real time interaction tool

In this vivid ecosystem users could easily keep truck of the information that others shared. Initially people used Facebook as a service that combined previously known internet services such as e-mails, blogs, instant online messages, address book etc. Users added personal information and material, such as photos, to their profile page and visited other users profile pages to be informed of any changes and comment on it. By News Feed, a service started in 2006, users could be informed of updates on other people's Facebook pages. Since March 2009 Facebook home page became of substantial importance for sharing information: As Chris Cox, Facebook's director of product development, has noted, the home page was redesigned, so as it would become a personalised newspaper of every user (Hof 2009). Users can easily attach their photos and videos, share their thoughts (by answering the question on top of their home page "what's on your mind"), publish their comments to material attached by others, link to other internet sources and communicate with friends by online instant messages without having to visit their profile page. Sharing information became much easier, its distribution more quick. Fast internet connections worldwide and also the service Facebook mobile, which enables users to have access to Facebook via their mobile phone, make possible for Facebook users to interact with their registered "friends" every second of their lives.

2.3 From "Web 2.0 for fun" to "Web 2.0 for productivity and services"

In 2009, Facebook creators realised that people tend to use Facebook not only for personal reasons. SNSs users may extend their networking communications beyond a purely personal or household activity, for example when the SNS is used as a collaboration platform for an association or a company (Art. 29 Working Party, 2009). Politicians use it as a forum to publish their political views, artists to show their work (paintings, music, video), scientists to share information etc. In March 2009 the Facebook was redesigned so as to accommodate all those different needs of expanding Facebook community users to one service. The first step was that *Pages* (used by companies, celebrities and professionals promoting their services) and *Profiles* (used by individuals) would become the same thing (Hof 2009). Business will also have the opportunity to have a Profile page, so it could be easier to interact with their customers and advertise new products and services. Those developments in Facebook are part of the new trend in social networks, a "shift from Web 2.0 for fun to Web 2.0 for productivity and services" (Art. 29 Working Party, 2009).

2.4 Facebook Users' information as business resourcee

In the expanding and borderless information market of Internet, users develop inevitably into an inexhaustible source of personalised information. Personal information - such as names, addresses, ages, marital status and family, employment and income status, shopping habits, websurfing habits, nationality etc. - is of enormous commercial value, particularly when used to create profile detail about "typical consumers" and then tailor marketing and advertising activities specifically towards the consumer's interests (Ciocchetti 2008, Hotaling 2008). Personal data published on social network sites can be used by third parties for a wide variety of purposes, including commercial purposes (Art. 29 Working Party 2009).

Facebook has searched for new models to take advantage of the accurate, detailed and updated users' profiles and information that company has access to. The Beacon application is designed to share information about a user's purschases or signed services activities on the Web sites of Facebook's commercial partners. Later, Facebook informs, via News Feed, the user's friends about her activities. According to its Privacy Policy (2008), Facebook disseminates aggregated data to other advertising companies and also it constitutes a Platform, where outside developers can built applications and have access to profiles for one day. In March 2009, Zuckerberg announced that Facebook is laying the groundwork for marketers to use Facebook in order to reach people in new ways. "A company, having a connection with a user has a real value", points out Mark Zuckerberg hoping that the number of connections could become a metric for marketing that goes beyond of impressions or clicks (Hof 2009).

3 CONSTRUCTING COMMUNITY TRUST OR A TRUSTED ENVIRONMENT?

Building a community presupposes constructing "community trust": a) trust between each user and the community, b) trust between the users/members of the community, c) trust between users and the company. A major difference Facebook has brought with was that trust between users is no more based on anonymity, pseudonymity or confidence among professionals. M. Zuckerberg, founder of Facebook, often describes Facebook as a "community", a group of people that trusted each other and the company, in which the company plays the role of "administrator". In Facebook communication environment, community trust is carefully constructed by the company, supported by architecture of Facebook applications and fed by social "needs".

3.1 Constructing users' community and trust

Facebook's Inc. primary and major goal was that users construct their own community of real life friends and acquaintances, using their real identity. Moreover, the construction and participation to such a community was a precondition to explore its services. In order to have access to many applications, the user had to invite at least a number of friends. A several number of applications required users to invite a number of their enlisted friends (usually twenty) in order to have the features of the application. In addition, Facebook through services like "Suggestions" and "Search Finder", initiates the expansion of those communities. Having new enlisted friends renews users' interest to Facebook and strengthens the commitment and perhaps the dependence on the website. Each bounded small Facebook community is the best advertisement of the social network site.

The construction of each Facebook community is often based on human courtesy. People find impolite to ignore people's invitation of becoming their "friends". Facebook's strategy is based on this. On the same time Facebook services do reflect social needs and, currently dominant, lifestyle. People use it as a forum, in which they can craft social identities, forge reciprocal relationships, and accumulate social capital (Grimmelmann 2009). Many users, especially youngsters, feel obliged to participate to SNS in order to have a social life.

SNSs and Facebook are grounded mainly on “self-exposure”, on the – cautious or incautious – decision of users to reveal information, sometimes even strict personal and sensitive, about their life. Furthermore, trust is based on mutual exposure. Facebook has developed into a powerful communicational tool because its users revealed their personal data. They revealed their data because their friends had first exposed themselves by adding photos and personal information. As Grimmelmann (2009 p. 19) notes “when we trust people, it’s often because of mutual surveillance, we’ll see if they betray us, and they know it, and we know that they know, and so on”. Constant communication creates an environment of intimacy (Ito, Okabe and Misa 2005) and trust between users.

3.2 Trust on Facebook and the promise of control over own’s information

Facebook users seem to trust website’s privacy policy and praxis. Facebook Inc. is aware of the fact that as the site is user-centered, its success and attractivity depend heavily on the number of users and the frequent usage of its services. So it is important to keep users’ trust and confidence to the company. Facebook accommodates its services to users’ requirements and needs. One of its core principles, laid down in Privacy Policy (2008) is that users should retain control over their personal information. Facebook informs users about the collection and processing of their IP address and the installation of a cookie with an opt-out choice. In addition, it informs users that third parties (developers of applications, company’s collaborators, public agencies etc.) could have access to their personal information. Facebook does send an alert everytime the user adds an application, noticing that a third company will have access to her data and friends’ data.

In addition, Facebook has one of the most comprehensive privacy management interfaces in relation to many other SNSs and websites. It provides sophisticated privacy settings. As Chris Kelly (2009), Facebook's Chief Privacy Officer, has stated on 1st July 2009, new privacy settings, initiated in July 2009, are grounded on three principles: control, simplicity and connection. Indeed, previous and new tools provide users with a number of possibilities: Every user can delete information she posted in her profile or her comments to other users photos or links, she can detagged her name from a photo attached by a friend etc. The user can choose, whether her friends, friends friends, every internet user or developers of applications can have access to her profile or information, which of her information will appear though public search in search engines like Google, what recent activity will be visible on her Profile and on her friends' home pages. She can also block someone from having access to her information.

However, a number of company’s choices, such as the introduction of News Feed (September 2006), the initiation of Beacon (November 2007), a new advertising system, in which users' purchases or activities on some 40 partner sites were broadcasted to their Facebook friends without user’s prior notice, and lately (February 2009) Facebook new terms of use have raised users’ protest and questioned their trust to Facebook’s policies. Facebook adjusted to those mass protests, adding privacy features in News Feed, giving at first opt-out choice and later opt-in choice for Beacon and restoring the old terms of service. Company’s next step was to create a Facebook Group and propose guidelines and a statement of rights and responsibilities. As Zuckerberg has stated, "rather than simply reissue a new Terms of Use, the changes we’re announcing today are designed to open up Facebook so that users can participate meaningfully in our policies and our future” (Carlson 2009). In April 2009 Facebook has announced that approximately 75 percent of users voted for the new terms of service. It seems as if Facebook accepts users as “network partners”.

4 EXPECTATIONS AND REALITY OF PRIVACY/ DATA PROTECTION

4.1 Privacy (in)awareness

Despite the choice – permitting privacy policy and the privacy settings it is highly questionable if users actually exercise control over their own information. A study of UK Office of Communications found that almost half of social network site users left their privacy settings on the default (Office of communications 2008). The new default privacy settings of Facebook include sharing profile picture, basic info, personal info, current location, education city, profile status, wall, notes, groups, events etc with developers of applications. Privacy default settings are based on half opt-out and half opt-in logic. It is as if Facebook proposes users to have a "quasi-public" profile. Behavioral economics scholars have demonstrated that individuals' general inertia toward default terms, specified by the vendor, is a strong and pervasive limitation on free choice (Korobkin 1998). Usually, even privacy-concerned Facebook users, do not read the privacy policy and those who claim they did, also had mistaken beliefs about how Facebook collected and shared personal information generally (Grimmelmann 2009). In any case, even when users change their default settings and choose to disclosure less or opt out from a service, they do not have many possibilities to find out if their preferences have actually been respected since the US law governing Facebook does not guarantee an effective exercise of a right to access to information retained by the company. Trust responds not necessarily to an adequate transparency

On the same time most users are unaware of the importance of sharing personal information. Users tend to misperceive Facebook as a private rather than a public space leading to unfortunate and unintended disclosures of personal and sometimes sensitive data (Edwards & Brown, 2009). They just add small isolated pieces of information about themselves. "One isolated piece of data about an individual is often not very revealing. Combining many pieces of information however begins to paint a portrait of one's identity" (Solove 2004). As a consequence if someone reads a two year profile of a Facebook user knows where she traveled, her mental and phychological state, if she is content with her life, her opinions about social or political events. Disregarding the warnings and disclaimers contained in Facebook's privacy policy, the majority of users tends to trust other users thinking they are «friends». But a large amount of information is shared with "friends' friends", i.e. strangers, which makes the subsequent control over the further uses of personal information quite impossible. Experience has proved that even careful users may find their data misused by third parties (Edwards &Brown 2009).The ability to control the terms of self-exposure in networked space seems to be largely illusory.

4.2 Privacy through regulatory and contractual instruments?

Established in California, Facebook Inc. has to comply with California Online Privacy Protection Act of 2003, which imposes internet companies the obligation to have a privacy policy, without providing specific legal obligations towards the users. Facebook Inc. has also adhered to EU Safe Harbour Privacy Principles, the agreement concluded between the European Commission and the United States Department of Commerce. This framework enables the free transborder flow of personal data from Member States of the European Union to organizations (established in US) that voluntarily join the above mentioned agreement, which consists mainly of seven privacy principles: notice, choice, onward transfer, control, security, data integrity, access and enforcement (Safe Harbour Principles 2000). Studies have revealed significant concerns regarding the compliance of several enlisted companies to seven principles (Connoly 2008). Facebook, as a licensee of the TRUSTe, an industry privacy seal programhas also to disclose its information practices and have these practices reviewed by TRUSTe, which has been criticized as "unsatisfactory" or, even, "untrustworthy" (Edwards & Brown 2009).

A significant question is whether SSNs providers established outside the European Union, like Facebook, are subject to the provisions of European data protection legal framework [Data Protection Directive (95/46/EC)]. In this case, Art. 29 Data Protection Working Party, which consists of the representatives of the national Data Protection Authorities of EU Member States grounds (Opinion 1/2008, Opinion 5/2009) the application of European Data Protection Law: a) on processing of personal data carried out in the context of the activities of an establishment of the provider within the EU and/or b) on the fact that equipment based within the European Union is used for the processing of data outside of it. Facebook denies the applicability of the European law arguing that it does not use such equipment, as cookie, and assuring that no personal data of Facebook users is processed in its international headquarters in Dublin or its offices in Paris and London. For European Data Protection Commissioners even the installation of cookies to the terminal equipment of European users from a provider established outside the EU is considered as "use of equipment" and invokes the European data protection legislation. Even if this approach has been criticized as "regulatory overreaching" in an online environment, it is undeniable that retention of IP addresses and use of cookies, constitute, if they allow the identification of the user, personal data processing under the terms of European law.

However, users enter – undoubdtly - voluntarily into Facebook, accepting its terms, conditions and privacy policy. SNSs, deemed to be "private spaces", are governed largely by consent and contract (Edwards & Brown 2009). Consent guarantees theoretically the right to express (freely taken) choices. Consent is given when a user signs up to Facebook. Users have the choice to opt between the privacy levels predefined and specified by Facebook but, actually their choice consists in "take it or leave it". Especially in the online environment, under the threat of "exclusion" from the "community" or denial of access to services and information, users consent without having any ability to negotiate terms and conditions (Ciocchetti 2008). Consent results in a "fallacy" for the individual (Schwartz 2000) or in an empty online ritual. Especially through the recently announced "Statement of Rights and Responsibilities", Facebook attempts to propose a "partner- quasi contractual, relationship between users and the company. However it is contestable if , under American law, this "privacy policy" constitutes an "agreement" or –simply – a "statement" (Hashemi 2009). In any case, such a "contract" would remain a standardized contract, characterized by a systemic disadvantage of individual users, as far as it concerns their bargaining and challenging powers and (in)abilities. Facebook still reserves the right to change its Privacy Policy and Terms of Use at any time (Facebook Privacy Policy 2008).

The crucial question remains: Isn' t an expression of individual autonomy to opt for self-exposure and "zero privacy"? Under the European privacy approach, based on dignity, one can freely dispose of one's liberty but can never be permitted to freely dispose of one's dignity (Rodota 2004). Moreover, apart from the information and power asymmetry of the "partners" and the contested ability of the users to control the use of information, our privacy concerns are nourished by the (in)ability, especially of young and experienced persons, to perceive and assess future risks of self-exposure.

5 FACEBOOK COMMUNICATIONAL ECOSYSTEM DECOSTRUCTS PRIVACY LAW

The discussion about rights and obligations, about the applicable regulatory and legal instruments is interrelated with the identification: a) of the nature of SNSs as public or private places and b) of users' activities in this context. Social networks blur the boundaries between personal sphere and public sphere. At the same time, in social networks the distinction between the powerful data controller and the vulnerable user (the "data subject" of European privacy law), which has served as the dominant scenario for establishing privacy rules, is not the only possible "conflict situation".

In U.S. privacy refers either to protection from government's intrusion upon individuals' privacy or to a privacy tort linked with the notion of control and the so-called property approach. In Europe, informational privacy protection is considered as a personality right but it is actually based on a

previous processing paradigm, where the infringer was easily recognised and data were collected for a specific purpose. Facebook shows how privacy is linked more with human interaction. In the context of SSNs and Facebook particular users can act not only as self-exposed individuals, giving up, exchanging or trading their privacy: Users are posting photos, comments, news, in the final analysis information not only about themselves but also about other persons, usually their enlisted friends but also non users of Facebook. Occasionally, they invade their friends' privacy: in UK Mr. Raphael set up a false Facebook profile for M. Firsht a formerly "close friend", containing private information, (including reference to his date of birth, relationship status, sexual preferences, and his political and religious views) as well as defamatory material. The Court ruled that Raphael should pay a total of GBP £22,000 (about USD $44,000) for libel and breach of privacy. [2008 EWHC 1781] .

Acting in a closed "friends community", users operate within a (purely?) personal sphere. However users are playing, at least potentially, a "central role in the collection, processing and distribution" of personal data (Wong & Savirimuthu 2008). This finding relates specifically to the European Data Protection Law. Users are acting as "data controllers" too and may become infringers of the rights and freedoms of other persons that are not necessarily users. If users use Facebook applications in order to contact other persons "as part of the management of their personal, family or household affairs" their activity remains "strictly personal" and falls in the scope of the so called "household exemption" of the EU Data Protection Directive (Art. 29 Working Party 2009). But what should be the answer if the number of contacts/friends is particularly "high"? A processing of personal data consisting in publication on the Internet so that data are made accessible to a wide or an indefinite number of persons cannot be considered as activity carried out in the course of private or family life [European Court of Justice Lindqvist-case C 101/01 (2003)]. And what happens if the user extends access to profile beyond the circle of selected friends? Or, when users use Facebook as a means to promote and achieve professional, commercial, political or charitable goals? In these cases, the European Data Protection Commissioners consider users as "data controllers" and affirm the application of the European Data Protection Directive, which imposes to them the obligations of data controllers (Art. 29 Working Party 2009). This approach, undeniably protective for the individuals, leads to serious problems and raises concerns regarding concerning the applicability and the enforceability of the law.

But is this unavoidable, exponential multiplication of data controllers and potential infringers the heart of the problem or disorientation from the "problem of privacy" in cyberspace and SNSs? A major issue to discuss is the changing personal and social attitudes concerning exposure, privacy and the use of information. Increased connectivity influences the perceptions of privacy and its relation to the free flow of information and its ready availability, which have been the original idea behind the Internet (Wong & Savirimuthu 2008). The discussion is not a theoretical one: Users' and society's understanding of privacy and its legitimate restrictions affect the meaning and the content of the "reasonable expectations of privacy", the prevailing method that the U.S. Supreme Court and other American Courts use to identify privacy rights and interests protected by the Fourth Amendment (Hodge 2007).The perception of informational privacy's content and boundaries influences also the interpretation of the "proportionality principle", a cornerstone of the European data protection approach, requiring necessity and appropriateness of processing measures as well as proportionality of purpose and means. In technology intensive societies the expectations of privacy or the perception of (dis)proportional information processing measures is inherently dependent on the actual stage of technological development.

6 LAST THOUGHTS AND DISCUSSION

Every person is principally free and entitled to make her own choices about revealing her personal information to others according to her experience, her judgments and wishes. However, we should not leave out of our consideration that the perception of privacy, the level and quality of privacy expectations of a Facebook user are highly formulated also by the architecture of online

communication and the "code" (Lessig 1999). Default settings as well as privacy settings may be used, in order to guide or manipulate users' perceptions of their control over software configuration (Kesan & Shah 2003). Facebook users are given half opt-out choices instead of giving an opt-in choice. Peoples' decisions about privacy may also be affected by the problem of the so-called bounded rationality, i.e when even aware and educated users have difficulties to apply what they know and decide in complex situations (Acquisti & Grossklags 2006). Therefore, Art. 29 Working Party (2009) stressed the importance of a) privacy-friendly default settings, which allow users to freely, specifically and explicitly consent to any access to their profile's content that is beyond their self-selected contacts and b) adequate information about purposes of data processing and warnings about privacy and security risks.

Facebook grows not as an ordinary social network but as an every day communication tool. At the same time marketing strategies such as *contextual marketing* (tailored to the content that is viewed or accessed by the user*), segmented marketing (through* advertisements to targeted groups of users) or *behavioural marketing* (based on the observation and analysis of the users' activity over time) are "an essential part of SNSs and Facebook business model" (Art. 29 Working Party 2009). However, this model should be redesigned in order to comply with users' privacy and consumers' protection regulatory imperatives. Without the elaboration of a new business model and privacy policies, based on free, conscious and informed consent of users about the future use of their data, information and power asymmetries may increase significantly in the new Facebook ecosystem to the detriment of the user, who won't have any control over her information but may be confronted with her past any time in the future (Pizzetti 2009).

References

Article 29 Data Protection Working Group. Opinion 4/2000 Article 29 Data Protection Working Party on the level of protection provided by the "Safe Harbor Principles" adopted on 16 May 2000. Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp32en.pdf (last visited 5/2/2008).

Article 29 Data Protection Working Group. Opinion 8/2008 Article 29 Data Protection Working Party on data related to search engines adopted on 4 April 2008. Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf (last visited 5/2/2008).

Article 29 Data Protection Working Group. Opinion 5/2009 on online social networking adopted on 12 June 2009. Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf (last visited 9/7/2009).

Acquisti, A. and Grossklags, J. (2006). Privacy and Rationality, in K. Strandburg and D.S.Raicu (Eds), Privacy and Technologies of Identity: A Cross-Disciplinary Conversation.

Acquisti, A. and Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, in Privacy-enhancing Tech.: 6th International Workshop 36 (George Danezis & Philippe Golle eds. 2006), Available at: http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook2.pdf. (last visited 2/5/2007).

Boyd, D. and Ellison, N. (2007). Social Network Sites (2007): Definition, History, and Scholarship, J. computer- mediated communication. 13(1) art. 11. Available at http://jcmc.indiana.edu/vol13/issue1/ boyd.ellison.html. (last visited 4/5/2008).

Carlson, N. (2009).We do not own the data users do. Business Week 26/2/2009. Available at http://www.businessinsider.com/zuckerberg-we-do-not-own-user-data-users-do-2009-2 (last visited 4/7/2009).

Ciocchetti, C. (2008). Just Click Submit: The Collection, Dissemination and Tagging of Personally Identifying Information. Vanderbilt Journal of Entertainment and Technology Law. Vol. 10 (Spring 2008), 553-642.

Connolly, C. (2008). The U.S. Safe Harbor- Fact or fiction 2/12/2008 Available at http://www.galexia.com/public/research/articles/research_articles-pa07.html (last visited 2/7/2009).

DiPietro, R. (2008). Constitutional limitations on public school's authority to punish student internet speech. Journal of Internet Law 12, 3-11.

Edwards, L. and Brown, I. (2009). Data Control and Social Networking: Irreconcilable Ideas?. Harboring data: Information Security, law and corporation, A. Matwyshyn, ed., Stanford University Press, 2009. Available at SSRN: http://ssrn.com/abstract=1148732. (last visited 3/7/2009).

European Network and Information Security Agency (ENISA). "Security Issues and Recommendations for Online Social Networks (2007).Available at: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf (last visited 5/6/2009).

Facebook Privacy Policy (2008). Available at http://www.facebook.com/policy.php?ref=pf (last visited 7/7/2009).

Grimmelmann, J. (2008). Facebook and the Social Dynamics of Privacy, New York Law School Legal Studies Research Paper Series 08/09 #7 Available at : http://ssrn.com/abstract= 1262822 (last visited 15/5/2009).

Hansell, S. (2008). Bits; Zuckerberg's Law of Data Sharing, 10. Nov. 2008 New York Times.

Hashemi, Y. (2009). Facebook's Privacy Policy and its third-party parthnerships: Lucrativity and Liability 15 B. U. Sci. & Tech L. 140-161 (2009).

Hetcher, S. (2008). User-Generated content and the future of copyright: Part Two- Agreements between users and mega-sites. Santa Clara Computer and High Technology Law Journal 24, 829-866.

Hodge, M. (2007). The Fourth Amendment and privacy. Issues on the "New" Internet: Facebook.com and MySpace.com, 31 S. Ill. U. L.J. pp. 95- 121.

Hof, R. (2009). Live: Mark Zuckerberg Lays Out Facebook's Next Moves. 4 March 2009 Business Week. Available at: http://www.businessweek.com/the_thread/techbeat/archives/2009/03/mark_zuckerberg_3.html (last visited 21/4/2009).

Hotaling, A. (2008). Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting. Commlaw Conspectus. Vol. 16. 529-565.

Ito, M. Okabe, D. and Misa, M. (2005). Personal, Portable, Pedestrian: Mobile Phones in Japanese Life. Cambridge: MIT Press.

Kelly, C. (2009). Improving Sharing Through Control, Simplicity and Connection posted 01 July 2009 Available at http://blog.facebook.com/blog.php?post=101470352130 (last visited 5/7/2009).

Kesan, J. P. and Shah, R. C. (2003), Deconstructing Code. Yale Journal of Law & Technology, Vol. 6, pp. 277-389, 2003-2004. Available at SSRN: http://ssrn.com/abstract=597543 (last visited 1/7/2009).

Korobkin, R. (1998). Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms. Vanderbilt Law Review. Vol. 51, 1583-.

Kushin, M. J. and Kitchener, K. (2009), Getting Political on Social Network Sites: Exploring Online Political Discourse on Facebook. Annual Convention of the Western States Communication Association, Phoenix, Paper. Available at SSRN: http://ssrn.com/abstract=1300565 (last visited 4/11/2008).

Lessig, L. (1999). Code and Other Laws of Cyberspace. eds. Basic Books New York.

Morganstern, A. (2008). In the spotlight: social network advertising and the right of publicity. Intellectual Property Law Bulletin Spring 12, 181-198.

Office of Communications, (2008). Social Networking: A quantitative and qualitative research report into attitudes, behaviours, and use. Available at: http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf (last visited 6/7/2009).

Polar, R. (2007) In the face of danger: Facial Recognition and the limits of privacy law, Harvard Law Review 120, 1870-1891.
Pizzetti, F. (2009). Is there a fundamental right to forget? Data Protection Conference "Personal data– more use, more protection?" , Brussels, 19-20 May 2009.
Rodota, S. (2004). Privacy, Freedom and Dignity – Closing remarks. Proceedings of 26th International Conference on Privacy and Personal Data Protection. Wroclaw.
Safe Harbour Principles (2000). Available at: http://www.export.gov/safeharbor/eu/eg_main_018475.asp (last visited 3/3/2009).
Solove, D. J. (2004). The Digital Person, Technology and Privacy in the Information Age. University Press, New York.
Schwartz, P. (2000). Privacy, Participation and Cyberspace – An American Perspective. D. Simon/P. Weiss (Hrsg.). Zur Autonomie des Individuums – Liber Amicorum Spiros Simitis. Nomos Verlag, Baden-Baden, 2000, 337-352.
Wong, R. and Savirimuthu, J. (2008). "All or nothing: the application of Art. 3.2 of the Data Protection Directive 95/46/EC to the Internet. John Marshall Journal of Computer & Information Law, Vol. 25, No. 2, Available at http://ssrn.com/abstract=1003025 (last visited 5/11/2008).