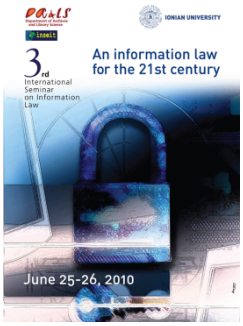
Privacy in the nook of Facebook

By
Marinos Papadopoulos
Attorney-at-Law, Managing Partner of
PATSIS, PAPADOPOULOS, KAPONI, & ASSOCIATES
(Attorneys-at-Law)
E: marinos@marinos.com.gr | **URL:** www.marinos.com.gr

&
Alexandra Kaponi
Attorney-at-Law
PATSIS, PAPADOPOULOS, KAPONI, & ASSOCIATES
(Attorneys-at-Law)
E: alexandra@marinos.com.gr | **URL:** www.marinos.com.gr



Abstract: In this work, we're approaching Facebook as a social networking site with the aim to understand the level of privacy and data protection related to it. This approach is affected by the sensitivity on the issue and regulation for data protection in effect in the E.U.

Keywords: Facebook, social networking sites, privacy, data protection law, personal data, sensitive data, privacy protective behavior, public living, Information disclosure, identity construction, Facebook Platform and Applications, "semi-public" or "semi-private", "friends", "information risk", "Privacy by Design", conversion tracking, social advertising, "behavioral targeting."

Privacy and information sharing in contexts of daily life with different norms

Information pertaining to the private sphere of one's life is not a fixed and undisputed meaning in law, but rather it is contextually defined in consideration of the social environment of one's life, the perceptions, mentations, customs of a certain social environmental context, which might be in constant flux. There are no areas of life not governed by context-specific norms of information flow, and privacy is not an exception to this rule. People move into and out of a plurality of distinct contexts

every day with a reasonable expectation for respect of their privacy, at least in Europe.[1] As we move between spheres of daily life, we have to alter our behaviors to correspond with the norms of those spheres, i.e. to adjust our behaviour to those spheres of daily life, but usually we do not deprive ourselves willingly from the right to privacy despite the fact which we easily acknowledge hastily that there will always be risks in information-sharing in the sense that information appropriately shared in one context becomes inappropriately shared in a context with different norms. Information is always tagged, as it were, with the context in which it is revealed, though in the E.U. legal framework, compares to the U.S. law,[2] there is more certainty upon to what information constitutes the core of privacy, personal and sensitive data and what the requirements are for legal use of it irrespective of the context that this information is used. Still, there is no such thing as context-free information; the protection of privacy makes sense both in public and in private spaces, and the meanings of privacy, public and private spaces are subject to different norms and contexts which are (re)shaped in society constantly.[3] For most of the people with no legal background, privacy and information-sharing related to it can probably better be understood in relation to the context in which information is shared.

In this work, we're approaching the context of Facebook as a social networking site with the aim to understand the level of privacy and data protection related to it. This approach is affected by the sensitivity and regulation for data protection in effect in the E.U.,[4] though we're aware of the fact that Facebook Inc., is not a legal entity based in the jurisdiction of any E.U.-member country,[5] but rather subjects to the U.S. law.; yet, it may also subject to the E.U. data protection law in accordance with the legal opinion of the Article 29 Data Protection Working Party.[6] That fact should not drive us into the conclusion that Facebook Inc., could organise and operate in consideration only of the U.S. law for data protection and privacy, but rather it should consider and organize its Facebook Platform and Applications with the aim to abide by E.U. data protection regulation.[7] Facebook represents a novel phenomenon to (risk of) data protection and privacy[8] online that considers all companies of the breed of social networking sites, probably because of the fact that Facebook is the most widely known and used[9] among them.[10]

In order to define social networking sites, we consider boyd[11] and Ellison's definition of them as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.[12] The defining characteristics of a social networking site are (a) tools for posting personal data[13] into a person's 'profile' and user-created content linked to a person's interests and personal life; (b) tools for personalised, socially-focused interactions, based around the profile (e.g.

recommendations, discussion, blogging, organisation of offline social events, reports of events); (c) tools for defining social relationships which determine who has access to data available on social networking sites and who can communicate with whom and how.[14]

Research findings and studies on Facebook users

Almost all of the evidence suggests that Facebook users primarily use the social networking site to solidify and develop their offline social relationships, rather than to make new relationships online.[15] Young people primarily use online technologies to talk with people they already know.[16] Facebook claims to have an age restriction for young people under 13 years old,[17] but this age restriction and website mechanism for age verification seems to be relatively effective. For an underage user it is quite easy to cheat the age-verification mechanism by making a false statement.[18] Website safeguards, which include content advisories, age verification, or credit card verification, were found to be reasonably effective at decreasing the amount of personal information provided by children 10-12 and 13-14, but not prohibitive for participation in the Facebook Platform and Applications, which means that children 10-14 years old were able to log onto the system by making false statements regarding their age; for 15-17 year olds, safeguards created a "boomerang effect" where teens reacted negatively, attempted to circumvent the safeguards, and ultimately tended to provide more personal information than when safeguards were absent.[19]

Although users' practice to put their information online in social networking sites is perceived to be a risk for harassment, solicitation, flaming,[20] denigration,[21] impersonation,[22] outing,[23] trickery,[24] exclusion,[25] stalking,[26] and threatening by revealing personal information,[27] people, especially young social networking sites users tend to flirt, gossip, build relationships and hang out with peers at social networking places online.[28] The more young people use the Internet to talk to their friends and engage in playful, social behaviour, the more likely that young people is to reveal personal information and the less likely to engage in privacy-protective behaviours.[29] Moreover, research indicates that Facebook users rarely change their default privacy settings, leading to the conclusion that users are "quite oblivious, unconcerned, or just pragmatic about their personal privacy."[30] Studies show that young people conceptualize the Internet as a private space where they can share secrets and talk to their friends, behaviour that intrinsically requires the sharing of personal information.[31]

This behaviour causes privacy worries which are centred on the risks of "public living" through social networking sites such as Facebook.[32] Constant publicity of Facebook users' data tends to cause them to modify their desires and behaviors accordingly so as to cope with the fact of being public and of having all of their data that is inferred onto the system being publicly available all the time.[33] The logic is: if everything in life is an image, then images become real for us, so we

tend to view ourselves in terms of the images we present, and tend to take pleasure in constructing the images of ourselves.[34] In addition, the perceived social benefits of online information-sharing seem to be perceived as outweighing any potential privacy risks.[35] The idea of being publicly and constantly available the constructed images of Facebook users on its platform at some point is in good terms with the idea of being under incessant surveillance—at least by the people who the users recognize as their friends—which causes people to stop hiding, and the panoptic principle is felt as neither a threat nor punishment, but, rather, as amusement, liberation and pleasure.[36] Information disclosure through Facebook and online popularity are interrelated and are inextricably linked. Disclosure thereby becomes an aspect of identity construction, and that construction is linked with popularity: the people who are most popular are those whose identity construction is most actively participated in by others.[37] As a result, the risks of limiting access to personal information become greater than the risks of disclosure, because when limiting access, the Facebook user also limits the potential for identity construction and thus potentially reduces his or her popularity through the Facebook Platform and Applications.[38]

Digital dossiers, data brokering of Facebook users' personal and sensitive data, and other threats to privacy

For many people the very distinction between "public" and "private" is problematic.[39] They tend to view privacy in more nuanced ways, conceptualizing Facebook spaces as "semi-public" or "semi-private" depending on the angle they look it from or making distinctions between different groups of "friends."[40] The urge to post as much private information on Facebook as possible with the aim to construct images of them[41] that are being constantly public is much closer to the need of Facebook users to seek publicity[42] rather than the need to protect their private information in a public forum.[43] Commercial data brokers like ChoicePoint[44] have leveraged on this need and made a (huge) profit by piecing together people's personal data to form individual profiles or "digital dossiers"[45] of people such as Facebook users who tend to put online as much personal data and information as possible.[46] Personal information is a commodity that is bought and sold by data-mining companies, marketing firms, and credit reporting agencies, and is especially valuable when coming from young people, whose consumption is a multi-billion dollar industry.[47]

The "digital dossiers" threat is not the only one, of course. There are others, too, which could result into lucrative data-mining and aggregation to the detriment of Facebook users' privacy and personal data protection.[48] ENISA has been looking at them carefully trying to shed light upon the phenomenon of social networking sites seen from the angle of information risk. Among these threats, ENISA includes the use of face recognition technologies,[49] Content-based Image Retrieval (CBIR) technologies,[50] linkability from image data,[51] difficulty to complete account deletion, SNS spamming,[52] Cross Site Scripting

(XSS) viruses and worms,[53] SNS aggregators,[54] SNS phishing, profile-squatting and reputation slander through identity theft, stalking,[55] bullying,[56] and corporate espionage. In the online forum of Facebook Platform and Applications, users, unaware of the existence of data brokers or data miners that gain from personal data exploitation and trade, have come to present themselves accordingly more in consideration of taking advantage of Facebook's enhanced and inevitable publicity rather than with the aim to protect the privacy of private information which is willingly posted onto a public forum. This behaviour has been the cause for increasing use and dissemination of personal information which could set data subjects increasingly powerless and vulnerable due to lack of control of their own personal information, images and reputation.[57]

Persistence, Searchability, Replicability, and Invisible audience

Information posted to the Internet is potentially visible to all. For most people, such universal broadcast of information has no parallel offline.[58] In other words, offline personal information is seldom communicated to a context anywhere near as broad as the entire Internet. Information flows on social networking sites such as Facebook are mediated not just by the global nature of Internet communication, but by the ways that those sites and their users interpret the meaning of online friendship and the social norms that go with it.[59] Boyd argues that social networking sites are complicating the way in which people interact because they have four properties usually not present in face-to-face public life:[60] *Persistence*: Unlike the ephemeral quality of speech in unmediated publics, networked communications are recorded for posterity. This enables asynchronous communication but it also extends the period of existence of any speech act. *Searchability*: Because expressions are recorded and identity is established through text, search and discovery tools help people find like minds. *Replicability*: Hearsay can be deflected as misinterpretation, but networked public expressions can be copied from one place to another verbatim such that there is no way to distinguish the "original" from the "copy." *Invisible audiences*: While we can visually detect most people who can overhear our speech in unmediated spaces, it is virtually impossible to ascertain all those who might run across our expressions in networked publics.

Also, according to Yochai Benkler, in the online context two general phenomena can be observed. First, "We see a thickening of preexisting relations with friends, family, and neighbors, particularly with those who were not easily reachable in the pre-Internet-mediated environment."[61] Second, "we are beginning to see the emergence of greater scope for limited purpose, loose relationships" as for example those surrounding topic-specific blogs.[62] Both these two phenomena exist in the Facebook environment. While in offline life privacy related to the cultivation of thick or loose relationships is a matter of face-to-face interactions and ad hoc decision making, in the environment of Facebook privacy can hardly become a matter to cope with on a case-

by-case basis, but rather is merely an issue that is left to manage through the system's available privacy settings and mechanisms. Although Facebook theoretically has a highly granular set of privacy settings, users do not appear to be taking advantage of them. Research indicates that the majority of Facebook users do not understand or even read the privacy statements.[63] Or that even those who read and understand them, do not refrain from posting their personal data and information online. Acknowledgment of privacy statements and settings does not affect information provision, suggesting that ignorance of privacy statements and settings is not wholly responsible for the reluctance of Facebook users to restrict access to their profiles.[64] It is beyond doubt, though, that when the privacy statements and settings are byzantine, difficult to find, and hard to understand, then this is a main reason for the existence of users' inability to form or effectuate their privacy preferences.[65] In addition, Facebook's structure as a system which encourages a binarization of social relations into "friend" and "not friend," flattens out all of the nuances of face-to-face interactions and all the options regarding privacy protection that is judged ad hoc in offline life.[66] Thus, even if assumed that Facebook privacy statements and settings had not been byzantine, even if Facebook users had not had any difficulty in understanding and using them, their privacy options would have been quite relative in effect simply because their privacy status would subject to their friends' privacy options, as well. And a Facebook user can never command what his/her Facebook 'friends' will opt to regarding their privacy issues as well as how the 'friends' will behave online regarding privacy protection.

Members of the Facebook community can create their own personal profile–complete with a profile photo and public photo albums, videos, and notes. They can also designate "friends," who are other Facebook users, and join virtual "Groups" that are focused around common themes and interests. Members can also choose which parts of their profile they would like to make visible to other members. Facebook also contains a "news feed," which is located on a user's Facebook homepage immediately after they log into the site. This personal news feed functions much like a typical news feed does. The basic difference is that the "news" contained in the Facebook news feed consists of profile updates made by a user's friends. Typical news stories include updates to relationship status, changes to information that members list about themselves on their profiles, and new photos that members have posted to their albums.

Facebook, that was set up by 2004, was initially only available to users who had a valid email address from a handful of colleges and universities. The site essentially served as an online, extended version of paper "facebooks" that are distributed at many college campuses to incoming freshmen. When it started, Facebook was a private space for communication with a group of a user's choice. By that time, a news feed on a user's friend could be seen only by said user. Soon, it transformed into a platform where much of a user's information is

public by default, thus a news feed could be seen by any Facebook user if the content posted online was set to 'Everyone' privacy settings. In 2006, Facebook was opened to all members of the general public. Today, it has become a platform where a user has no choice but to make certain information public—'Everyone' information—and this public information may be shared by Facebook with its partner websites and used to target ads. Today, the only membership requirements are a valid email address and formal agreement to the website's Terms of Use and Privacy Policy.[67] Facebook can now gather unprecedented amounts of personal information on its users. While information disclosed is ostensibly used by Facebook to customise and personalise its services, it can also be used for targeting (e.g. advertising), discrimination (e.g. price discrimination) or the transfer of data to third parties through resale.

Facebook Applications

In May 2007, Facebook introduced their application platform, allowing third party developers to create added functionality that links to a user's profile. These applications enhance the social experience on Facebook by allowing users to add additional content to their profiles, play games with their friends, share photos and other media, and much more. The main three features that Facebook added to its social networking system involving partnerships with third parties were Public Search, Social Ads, and Beacon. Theses applications have been extremely successful. Facebook reports that 70% of users interact with an application each month, with over fifty thousand applications available.[68] In order to complement a user's profile, Facebook allows applications to access most of the user's profile information, except for contact information. More disturbing, however, is that these applications are also allowed to access the same information for all of a user's friends! While this allows applications to incorporate information about a user's social spheres into their functionality, few need access to such a wide variety of information to do so.

The privacy problems with such applications are easy enough to see.[69] If I join a fitness club, I expect to tell them my name and address, as well as some information about my fitness level and maybe even my doctor's name or my birthday. I do not expect to share which books and movies I like, where I went to school and where I work, and what my religious and political affiliations are or what is my sexual orientation by answering any kind of direct or indirect questions upon it. And my friends have every reason to expect that I will not share the parallel information about them with the fitness club.[70] This information sharing is largely invisible, despite the fact that Facebook self-describes its nature of operations as a mechanism that is about sharing information with others either friends or other members in the Facebook community.[71] Users are alerted with a simple message each time they install an application that both their own and their friends' information will be shared. However, this message is not very descriptive, and is easy to ignore as users are more focused on the task of using the

application than on their privacy. Many users simply 'click through' these privacy notices, ignoring the one important piece of information that alerts them about giving away their information and the information of their friends to third parties.

Facebook's incremental transformation

Facebook's incremental transformation regarding its privacy policy is indicative of the company's profitable manoeuvres in association with its advertising and business partners leveraging on the valuable personal data and information of its users.[72] Facebook originally earned its core base of users by offering them simple and powerful controls over their personal information. As Facebook grew larger and became more important, slowly but surely leveraged more and more on its users' information and personal data with the aim to profit from business partnering and advertising in exchange for sacrificing of privacy and data protection and for limiting Facebook users' options to control their own information.[73] EFF's presentation of Facebook's Privacy Policy timeline indicates gradual withdrawing from strict data protection and privacy of personal information submitted to the system by its users.[74]

Facebook Privacy Policy circa 2005: "*No personal information that you submit to Thefacebook will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings*."

Facebook Privacy Policy circa 2006: "*We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your school, your specified local area, and other reasonable community limitations that we tell you about*."

Facebook Privacy Policy circa 2007: "*Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings.*"

Facebook Privacy Policy circa November 2009: "*Facebook is designed to make it easy for you to share your information with anyone you want. You decide how much information you feel comfortable sharing on Facebook and you control how it is distributed through your privacy settings. You should review the default privacy settings and change them if necessary to reflect your preferences. You should also consider your settings whenever you share information. … Information set to "everyone" is publicly available information, may be accessed by everyone on the Internet (including people not logged into Facebook), is subject to indexing by third party search engines, may be associated with you outside of Facebook (such as when you visit other sites on the internet), and may be imported and exported by us and others without privacy limitations. The default privacy setting for certain types of*

information you post on Facebook is set to "everyone." You can review and change the default settings in your privacy settings."

Facebook Privacy Policy circa December 2009: "*Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings. You can, however, limit the ability of others to find this information through search using your search privacy settings.*"

Current Facebook Privacy Policy, as of April 2010: "*When you connect with an application or website it will have access to General Information about you. The term General Information includes your and your friends' names, profile pictures, gender, user IDs, connections, and any content shared using the Everyone privacy setting. ... The default privacy setting for certain types of information you post on Facebook is set to "everyone." ... Because it takes two to connect, your privacy settings only control who can see the connection on your profile page. If you are uncomfortable with the connection being publicly available, you should consider removing (or not making) the connection.*"

Criticism by the E.U. Article 29 Data Protection Party

Facebook's said withdrawal from strict data protection and privacy policy was severely criticised by E.U. data protection Authorities such as the Article 29 Data Protection Working Party which considers unacceptable the fact that the company fundamentally and incrementally changed the default settings on its social-networking platform to the detriment of a user's privacy and emphasises the need for a default setting in Facebook Privacy Policy in which access to the profile information and information about the connections of a user is limited to self-selected contacts. The Article 29 Data Protection Working Party considers that any further access to Facebook users' personal data and information, such as by search engines, should be an explicit choice of the user; additionally any use of personal data of other individuals contained in a user's profile in Facebook Platform for commercial purposes should be subject to the prior free and unambiguous consent of the data subjects as said consent is defined in E.U. data protection legislation.[75]

The Fourth Amendment protection and the Third Party doctrine

A significant legal consequence of the voluntary sharing of people's information through Facebook and other social networking applications is that information "knowingly exposed to the public" is not entitled to privacy protection through the application of the Fourth Amendment protection in the U.S. law.[76] Which means that Facebook Inc. based in the U.S. and subject to the U.S. law primarily is not bound by the restrictions regarding privacy protection for the users of Facebook Platform and/or Facebook Applications. Where information is voluntarily shared with another party, it may be legally obtained by any third party even any

Governmental agency and without a warrant.[77] Therefore, people should have no reasonable expectation of privacy in data they give to third parties such as Facebook Inc., and/or other entities through Facebook Platform and/or Facebook Applications. This standard applies equally to information truly open to the public as well as information voluntarily shared with a third party within the context of a confidential relationship, such as a business.[78] When a person reveals private information to a third party such as Facebook Inc., that individual "assumes the risk" that the third party may reveal the information to authorities (the "third-party doctrine").[79] If the third party willingly reveals that information to the authorities, the Government and any government agency do not violate the Fourth Amendment by using it.[80] And it is doubtful whether any legal protection against them regarding said data-mining practice for investigative, surveillance or any other purposes through social networking sites can be sought, even if it's based on the Freedom Of Information Act (FOIA)[81] of the U.S.[82] Not only that is true and sustainable, but also the fact that Facebook (as well as any other social network site) can be subpoenaed by a U.S. government agency[83] with the aim to provide it a Facebook user's account information and any other personal data submitted to the Facebook Platform and/or Applications by the user or any third party, even if that account is locked based on privacy settings.[84] Moreover, it should be noted that it's not only Government and government agencies such as law enforcement agencies (e.g. F.B.I.) that are not bound by the Fourth Amendment protection regarding the use of information found and retrieved through Facebook Platform and/or Applications. Employers,[85] school districts, insurance companies, direct marketing companies and corporations can and do use freely social network sites in order to collect information about prospective hires, potential law-breakers, criminal acts, students, risky behaviours, and consumer behaviour.[86]

Trust in Privacy by Design v. Publicity by Design

In consideration of the application of the "third-party doctrine" of U.S. law in the case of Facebook Privacy Policy, it makes without saying that Facebook's evolving privacy policy is architecture for publicity rather than privacy. If this is a given, then Facebook's evolution seems to be in direct confrontation with the conceived need for promotion of trust in the Information Society by fostering data protection and privacy in the European market. Contrary to what is the situation in the U.S. wherein Facebook Inc. is based, in the European market individuals are at the core of the new environment of ICT and Information Society online, and an individual's privacy is protected even when personal data is submitted to any Governmental organization or any organization within the Public Sector.[87] In Europe individuals must be able to rely on ICT's ability to keep their information secure and control its use, as well as be confident that their privacy and data protection rights will be honoured in the digital space. Respect of those rights is essential in order to generate consumer trust. And such trust is crucial if citizens are to embrace new services.[88] A

lack of trust in the online environment is seriously hampering the development of Europe's online economy. Among people who did not order any products or services online in 2009 and among the top reasons about it were privacy concerns, and trust concerns.[89] This envisaged trust which is of crucial importance in the E.U. online environment must satisfy the need to integrate, at practical level, data protection and privacy from the very inception of new information and communication technologies which is referred to as the principle of "Privacy by Design."[90] The right to privacy and to the protection of personal data are fundamental rights in the E.U. which must be also online effectively enforced using the widest range of means: from the wide application of the principle of "Privacy by Design" in the relevant ICT technologies, to dissuasive sanctions wherever necessary. The E.U.'s revised legal framework for electronic communications clarifies the responsibilities of network operators and service providers, including their obligation to notify breaches of personal data security. The recently launched review of the general data protection legal framework will include a possible extension of the obligation to notify data security breaches.[91] Yet, despite this European will to reinforce the "Privacy by Design" principle in the E.U. market for the sake of trust in the ICTs and Information Society, Facebook's current Privacy Policy seems to favour the opposite, i.e. unprecedented, unrestrained, and unexceptional "Publicity by Design" rather than "Privacy by Design," thus seems to be out of context with the legal framework for data protection and privacy in the E.U.[92]

Criticism by the E.U. Data Protection Supervisor

For this reason, the European Data Protection Supervisor has identified social networking sites such as Facebook—among other Internet applications such as RFID technology—that deserve careful consideration by the European Commission regarding data protection and privacy. Facebook as a social networking service is considered data controller insofar as it provides the means for the processing of user data and provides all the basic services related to user management.[93] In legal terms this means that Facebook users and Facebook Inc., share joint responsibility for the processing of personal data as "data controllers" within the meaning of Article 2(d) of the Date Protection Directive, albeit to different degrees and with different sets of obligations.[94] In the opinion of the E.U. Data Protection Supervisor, Facebook users by processing their personal information and that of others, they fall under the provisions of the E.U. legislation on data protection that requires, among other things, obtaining the informed consent[95] of those whose information is uploaded and granting those concerned with the right of rectification, object, etc. Similarly, Facebook as a social networking service must, among other things, implement appropriate technical and organisational measures to prevent unauthorised processing, taking into account the risks[96] represented by the processing and the nature of the data. This in turn means that Facebook as well as other social networking sites should ensure privacy-friendly default settings, including settings that

restrict profile access to the user's own, self-selected contacts. Settings should also require user's affirmative consent before any profile becomes accessible to other third parties, and restricted access profiles should not be discoverable by internal search engines.[97] However, Facebook preselects default settings based on opt-outs, thus facilitating the disclosure of personal information by default. Its current Privacy Policy enables profiles to be available to common search engines by default and considers certain categories of personal information as "Everyone" information that does not have any privacy settings and protection.[98] This raises questions as to whether individuals have actually consented to disclosure, as well as whether social networks have complied with Article 17 of the E.U. Data Protection Directive (described above) requiring them to implement appropriate technical and organisational measures to prevent unauthorised processing.[99]

'Everyone' by default

When Facebook was initially opened, only members could search for other members. On September 5, 2007, Facebook announced that it had made limited public search listings available to people who are not logged into the Facebook website. These search listings expose members' names, profile pictures, the ability to send a message to a member, view his or her friends, and request to add that member as a friend.[100] Facebook also announced that it will make these listings available on search engines such as Google, MSN Live, and Yahoo, which of course, soon after September 5, 2007, did happen.[101] Facebook did not send any email notices to its users notifying them that their listings had become publicly available and or that Facebook users' information is set to 'Everyone' by default. Indeed, Facebook announced through its blog that it does not have a policy of notifying users of changes to the site via email.[102]

Carolyn Abram, Facebook's "resident blogger," explained there are only four ways that Facebook sends information to users[103]: through Home Page announcements, Product Stories and the What's New page, the Facebook Blog, and Pages and Updates. Home Page announcements are "big boxes" that appear at the top of a user's News Feed when that user logs into Facebook. Abram explained that Home Page announcements are used only for the announcements that Facebook wants to be sure its users are aware of.[104] Product Stories and the What's New page appear as stories on users' News Feeds and are used to communicate "useful tips and fun information about Facebook." Finally, Pages and Updates appear in users' message inboxes, which they can access after logging into the website. After the public search change that Facebook Inc., decided arbitrarily, all users were automatically included in the public search listings; they were given the option to opt-out of the public listings, but of course said option was offered after the fact of being publicly listed, via Facebook's individualized privacy settings page.[105] Before Facebook's move to make its search listings public and available on search engines such as Google, MSN Live, and Yahoo there had been no amendment to

Facebook's privacy policy to cover the implications of public searches, but rather only a phrasing included in the Facebook principles[106] stating that "*Please keep in mind that if you disclose personal information in your profile or when posting comments, messages, photos, videos, Marketplace listings or other items, this information may become publicly available*."[107]

Currently, Facebook Privacy Policy specifically notes that user information may be made public. It states that "*Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings. You can, however, limit the ability of others to find this information through search using your search privacy settings*."[108] And it also reminds its users that "*Some of the content you share and the actions you take will show up on your friends' home pages and other pages they visit. If another user tags you in a photo or video or at a place, you can remove the tag.*" But this tag-removing activity can, of course happen only after the photo is already published. It also states that "*You can also limit who can see that you have been tagged on your profile from your privacy settings.*" But this limitation is not applicable to a photo published by a friend of a user who has opted for different privacy settings than the user's settings.[109] Facebook explicitly admits that "*Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings, or it was copied or stored by other users*." That is to say that information removal might be totally ineffective for a user since in almost all cases postings of information in one place are viewable in many others, and users tend to re-post elsewhere information they like.[110] And that a user understands "…*that information might be reshared or copied by other users.*" And since a user understands this as a standard process and still consents to the use of the Facebook Platform, there's limited room to object to it through any applicable and sustainable legal action against Facebook Inc.

Facebook's decision to make public search listings available initially generated some user protest,[111] but that protest quickly waned.[112] This may be because creating a profile, which gives access to Facebook user information, requires so little effort. Because establishing membership is very easy, many members do not see a fundamental difference between opening Facebook up to public membership, and allowing non-members to search Facebook profiles. However, Facebook's announcement that it would make public listings available to users of search engines was a dramatically new and unprecedented development in the world of social networking websites.[113] It may not be a decision that members felt they agreed to when they read and accepted the website's privacy policy.[114] Yet, their protests against making listings publicly available were not loud enough to make Facebook Inc. retreat

from putting their users' personal and sensitive data at anyone's access and retrieval.

Additionally, the developers behind the Facebook applications are also largely invisible, obscuring the fact that the information is in fact leaving the confines of Facebook and not just going to the user's friends. Applications run within the boundary of the site, giving users the impression that they are interacting with Facebook and others on Facebook.[115] Yet, this effectively obscures the fact that they are also interacting with some third party server on which Facebook Inc. and Facebook Platform have no power and probably the Facebook application developer has no full power upon, too.[116] Moreover, users are not aware of the fact that all of the other personal information on their profile as well as personal and sensitive data and information of their friends' profiles are potentially being accessed by those third party application developers for who Facebook Inc. waives its legal responsibility acknowledging bluntly in fact the company's inability to control the behaviour of third party Facebook Application developers regarding the use of Facebook users' personal and sensitive data and information.[117] The result is that users have little understanding of the information they are sharing, with whom they are sharing it, and that they are responsible for sharing—leaking, actually—all of their friends' personal and sensitive data and information as well.[118]

Invisibility of information flows via Facebook

Facebook Privacy Policy provisions clearly indicate that any information members provide may become "publicly available." Facebook users do not have a subjective expectation of privacy in their profiles, since the very purpose of creating a Facebook profile is to make information available to others. Even though the privacy policy may not be a binding agreement, it still seems odd for a Facebook member to expect notice before his or her information is made publicly available when all members are required to agree to a privacy policy that specifically states that user information may be made publicly available. The invisibility of information flows presents a particular problem because when a user does not know what is being done with her information, she has no ability to contest it. If the architecture and interface of Facebook essentially hides the amount of information that is shared to third parties, then there is little that a user can do about that sharing.

Indeed, there is little that she can do to avoid the situation, other than decline to use the third party applications or Facebook per se. The choice for a user is binary: install the application and give full access to her own and her friends' personal information, or don't use the application at all.[119] If a user opts for installing a Facebook application then said user technically consents to participating in Facebook and the certain Facebook application when she signs up. But is questionable whether that consent is adequate in terms of the Law, especially in consideration of the meaning of consent in data-protection E.U.-

members regulation. Especially, one of the issues will be whether the consent was obtained under circumstances where the user understands what she's agreeing to.

New behavioral problems and the "shrinking perceived audience"

In addition, Facebook's architectural design poses us with new behavioural problems which seem to be quite difficult to cope with and come to a satisfactory solution leveraging on any data-protection legislation either in the U.S. or in the E.U. In offline life when dealing with a friend or a small group of them we tend not to perceive said friend or friends as being a number of a much bigger group of friends and peers. Instead, we focus on them and share personal data, beliefs and experiences with them with the perceived assurance that this friendly interaction is bounded by the limits of the participating friends. This behavioural norm affects friendly interactions in the online environment of Facebook, too, despite the fact that Facebook environment is totally different to offline friendly reciprocal communication. Though users tend to shake-hands with as many Facebook friends as possible, they also tend to operate periodically with a limited number of them in mind. One can hardly cope with some hundreds or thousands of friends daily regarding personal information and matters other than business and professional activities. After all, one's own life is not an issue to discuss with hundreds or thousands of people simultaneously unless said person is a public persona. Thus, most Facebook users tend to operate with a "shrinking perceived audience."[120] That is, they initially begin by friending a large number of people, and assuming that everything they say is more or less public. Most Facebook users tend to accept friend requests without checking their authenticity or suitability.[121] Over time, though, and as their active in mind circle of friends narrows, they tend to forget about the earlier friends, who are still active in the Facebook Platform and/or Applications, and tend to focus on the narrower cycle of the active friends only, but even when acting with them in mind, neither do they tend to perceive that their Facebook postings is a topic for discussion among all of their active—in mind, moreover in Facebook Platform—friends nor that any updates to their earlier discussions remain available permanently to be seen and used by any of their Facebook friends. The News Feed format also encourages this thought, since updates show up on one's list, only to be displaced shortly thereafter by other updates. One's experience, then, is of ephemeral news postings, not a permanent record. But the record is nonetheless permanent by default;[122] it is possible to go back and view all of a person's updates over a period of several years unless she deletes them.[123]

The behavioural norm of offline friendly interaction is a pattern that crops up subconsciously because it is manageable. Yet, this norm of offline friendly interaction is not a pattern applicable to the online environment of Facebook as we've presented hereto. Every posting of a user becomes public to a user's friends either they are active or not.

Thus, every personal data, and every newsfeed from a user's personal and/or professional life becomes a topic for discussion for any user's Facebook friend. Additionally, Facebook's architectural design aims at promoting multilateral rather than bilateral communication. Facebook's multilateral communication technologies and their interfaces can facilitate some values and behaviors at the expense of others such as one-to-one communication. Even when communication feels to be bilateral, in fact it is not. For example, 'wall-to-wall' communications allow one to exhange messages with a single friend asynchronously in what feels and looks like a private space, but which is in fact visible to others. The abstraction involved in asynchronous, online social networking encourages a gap between a user's perceived audience and the actual audience. Users tend to significantly under-perceive the size and scope of the audience for their postings.[124] The multilateral communication of Facebook's architectural design is constantly evolving as the technology of social networking sites enables entire types of interactions that are not available offline. Changes in the interface affect how people behave online, and those behavioral changes feed back into the norms that guide them.

Facebook Social Ads

Among the applications that were announced[125] in 2007 with the aim to enhance Facebook's social networking experience was what it called "an entirely new advertising solution for Facebook", i.e. Social Ads. Social ads display relevant advertisements related to actions that users have taken on the site.[126] The announcement specified that the new Social Ads product would result in three main changes for Facebook users: (1) it would give users a way to connect with "*products, businesses, bands, celebrities and more*"; (2) ads would become "*more relevant and more meaningful*" to users; and (3) users would have the options to share actions they take on third-party websites with their Facebook friends. Facebook assured users that advertisers would never have access to who is seeing their ads, personal information about users, or the social actions that accompany their ads, but rather that only friends of a user would share the personally identifiable information visible in a social ad.[127] This announcement was only published in the Facebook blog, though in accordance with Facebook policy, no announcements were sent to users' personal email addresses.[128] Also, though Facebook Inc. acknowledges data sharing, commonly known as "conversion tracking"[129] that helps the company to measure its advertising effectiveness and improves the quality of the advertisements that Facebook users see, it does not provide through the Facebook Privacy Policy any clarification upon the method it uses in the conversion tracking process.[130] And though Facebook Inc. states that it does not share its users' personal data with advertisers, yet it does state that the company allows advertisers to choose the characteristics of users who will see their advertisements through Facebook based on any of the non-personally identifiable attributes[131] of Facebook users that Facebook Inc. has collected and shared with advertisers including information that users may have decided not to show to other users,

such as their birth year or other sensitive personal information or preferences.[132] It is obvious that Facebook Inc., despite any different claims, it does leverage on personal data and information submitted to Facebook Platform by its users with the aim to profit from the exchange of this information. There are advertising methods such as the 'behavioral targeting' which are used in order to produce the maximum financial gains for the (right)-holder of this information.[133] Personal and sensitive data and information submitted into the Facebook system is treated as if it were a corporate asset; software development is using said data and information with the aim to make the most out of it, as well as make most users submit through the Facebook Platform as more data and information as possible.

Problematic and biphasic privacy in the nook of Facebook

In consideration of the analysis described hereto, it is beyond any doubt that privacy in the nook of Facebook currently is problematic and biphasic, at least. Biphasic is in the sense that by 2005 it started as data and information available to no one but a user and his/her friends unless said user decided otherwise, while by 2009 it turned into data and information available to everyone unless a user decided it to be only for him/her and his/her friends. And problematic is in any E.U. sense of privacy and data protection. Facebook's disrespect for privacy norms is reflected in the company's chief executive officer's publicly stated views. Facebook's founder and CEO Mark Zuckerberg has no hesitation in making public statements of his views that the age of privacy is over[134] or that what people want isn't complete privacy[135] or that he sees no reason why information in people's accounts, as in his own Facebook account, should not be public and accessible to everyone,[136] or in making assertions that people may be more excited about exposing their life-activities such as shopping records in a few years rather than keep these activities under the privacy hood.[137] Yet, he does recognize that privacy is an issue of focal point for Facebook.[138]

The current situation in Facebook is one of legal uncertainty—if not of legal confrontation and direct breach of data protection law in the E.U. legal environment—which causes problems for both regulators and individuals whose privacy and personal data are not fully protected.[139] Because of this fact as well as in consideration of the fact that national Authorities[140] as well as international European Authorities[141] have already pointed out the conflicts of social networking sites and practices with the local and the E.U. data protection legal framework with the aim to make Facebook and other social networking sites to comply with the local and the E.U. data protection law,[142] in my opinion Facebook Inc.—the biggest and most popular social network operator—is faced with an eerie, major, and multi-dimensional crisis. The first signs of this crisis for Facebook Inc. are already discernible through the press and the media.[143] Facebook is met more-and-more with bud publicity periodically regarding data-protection and privacy through the company's Platform and third-party Applications.[144] If the management

of Facebook Inc. does not decide to change its current Privacy Policy and reshape the Facebook Platform and/or Applications accordingly so as to comply with data protection legal frameworks that put an emphasis on the protection of individual's privacy rights, i.e. to provide settings that restrict access to Facebook users profiles to a user's own self-selected contacts, as well as settings that require user's affirmative consent in the meaning of prior free and unambiguous consent of the data subjects as said consent is defined in E.U. data protection legislation before any profile is accessible to third parties; if they don't opt for settings that provide restricted access to users' profiles so that they are not discoverable by internal/external search engines. If not that minimum but necessary for data protection and privacy compliance changes do not happen any time soon, if not Facebook Inc. make all necessary changes in its Platform and third-party admittance Applications policy so that users have full command of their personal data and information, then Facebook Inc. would probably have to face a litigation spree, that is to say legal measures with possible severe consequences, taken against it either by national Authorities, European Authorities or E.U.-members' Authorities and/or Facebook users in the form of class action suites, too. For Facebook Inc., a possible implication of this kind is not only a crisis of litigation nature, but could possibly, also, turn into a public relations and corporate public affairs crisis regarding the company's reputation and other intangible assets of it with negative consequences on the company's tangible assets and their traded value.[145]

The value of Facebook lies not just in the content provided (which is group-specific), but in its replication in electronic form of the web of human relationships and trust connections. Therefore, possible litigation based on breaches of privacy and data-protection legislation is a direct hit to the core of trust-relationships and connections which Facebook Inc. purports to support, and which is a necessary ingredient in the Information Society.[146] Facebook and all social networking sites may be seen as informal but all-embracing trusted identity management tools,[147] defining access to user-created content via social relationships. If this identity management were found to fail and mistrust because of privacy and data-protection failure, then the identity management tools operator would reasonably be expected to fail and mistrust, too, unless serious effort were undertaken with the aim to comply with data protection legal frameworks in consideration of which the identity management tool operator could be judged. Said legal frameworks may also need to be modified or extended aiming at ruling clearly the operation of Facebook and other social networking services which represent a relatively novice phenomenon.[148] Especially, differing legal frameworks which affect the operation and development of social networking sites through their provisions for the protection of privacy, personal and sensitive data of data subjects, such as the U.S. from one side and the E.U. from another, might need to be re-examined with the aim to adopt unified ruling on basic privacy, data protection principles and core data subject's rights. Negotiations aiming at that point have

already started between the E.U. and the U.S.[149] There is no doubt that Facebook and the peer social networking sites present a scenario, which was hardly foreseen clearly when current data-protection legislation was created. This means that certain issues in data-protection law may, also, need to be clarified.[150] But, it also means that Facebook Inc. under current legislative framework for data protection and privacy certainly needs to change its Platform and Applications so that it abides by law. It remains to be seen.

ENDNOTES:

[1] Mitrou, L., (2010), *Protection of Privacy in Information and Communication Technologies—The Legal point of view*, in Protection of Privacy & Information and Communication Technologies—Technical and Legal issues, Labrinoudakis, K., Mitrou, L., Gritzalis, S., Katsikas, S., eds., Papassotiriou publications; Mitrou, L., and Karyda, M., (2006), *Employees' Privacy vs. Employers' security: can they be balanced?*, Elsevier, Telematics and Informatics 23(2006); Slobogin, C., (2002), *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, Mississippi Law Journal 72(2002), available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=364600 [last check, Jun.5, 2010].

[2] Bygrave, L., (2004), *Privacy Protection in a Global Context—A Comparative Overview*, Published in Scandinavian Studies in Law, 47(2004), 319-348, available at http://folk.uio.no/lee/publications/Privacy%20in%20global%20context.pdf [last check, Jun.5, 2010]; Whitman, J., (2004), *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale Law Journal 1151 (2004), available at http://www.yalelawjournal.org/images/pdfs/246.pdf [last check, Jun.5, 2010].

[3] Nissenbaum, H., (2004), *Privacy as Contextual Integrity*, Washington Law Review 79, 101-139, available at http://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf [last check, Jun.5, 2010]; Hull G., Lipford H. R., Latulipe C., (2009), *Contextual Gaps: Privacy Issues on Facebook*, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1427546 [last check, Jun.5, 2010]; Cohen, J.E., (2000), *Examined Lives: Informational Privacy and the Subject as Object,* Georgetown Public Law Research Paper No. 233597, available at http://ssrn.com/abstract=233597 [last check, Jun.5, 2010]. For the extended and (re)shaped meaning of privacy in public and/or in private spaces, see Mitrou, L., (2010), ibid.

[4] In Europe, the protection of individuals with regard to the collection, processing, use and movement of personal data is covered by the European Parliament and Council

Directive 95/46/EC of October 24, 1995, or the Data Protection Directive (Directive 95/46/EC of the European Parliament 1995) (See the Data Protection Directive at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf [last check, Jun.5, 2010]). The processing of personal data and the protection of privacy in the electronic communications sector are the subject of Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, or the Directive on Privacy and Electronic Communications (Directive 2002/58/EC of the European Parliament 2002) (See the Directive on Privacy and Electronic Communications at http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf [last check, Jun.5, 2010]), which extends privacy protections to unsolicited commercial e-mail, telephone communications, requires websites to disclose the use of cookies, and recommends that privacy notices are short and easy for consumers to understand. The Directive on Privacy and Electronic Communications was amended by Directive 2009/136/EC of the European Parliament and of the Council of November 25, 2009 See the Directive 2009/136/EC at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF [last check, Jun.5, 2010]).

[5] Facebook Inc., is based in the State of California. The international headquarters of Facebook is based in Dublin wherefrom Facebook Inc., will provide a range of online technical, sales and operations support to Facebook's users and customers across Europe, the Middle East and Africa. The company refrains from clarifying what is the nature of said support and the services provided to E.U. citizens from its international headquarters in Dublin. See more at Press Release, *Facebook to Establish International Headquarters in Dublin, Ireland*, October 2, 2008, available at http://www.facebook.com/press/releases.php?p=59042 [last check, Jun.5, 2010].

[6] Facebook Inc. subjects to the E.U. data protection law because of article 4 of the E.U. Data Protection Directive (Directive 95/46/EC) and according to Article 29 Data Protection Working Party's interpretation of said clause. Article 4 of the Directive reads as follows: §1. *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; (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.* §2. *In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions, which could be initiated against the controller himself.* Also, see Article 29 Data Protection Working Party, *Opinion 1/2008 on data protection issues related to search engines, WP 148/00737/EN*, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf [last check, Jun.5, 2010]; the same, *Working document on determining the international application of E.U. data protection law to personal data processing on the Internet by non-E.U. based websites, WP 56/5035/01/EN/Final,* available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf [last check, Jun.5, 2010].

[7] Birnhack, M., (2008), *The EU Data Protection Directive: An Engine of a Global Regime,* Computer Law & Security Report, Vol. 24, No. 6, 2008, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1268744 [last check, Jun.5, 2010]; Burk., D., (2005), *Privacy and Property in the Global Datasphere*, Minnesota Legal

Studies Research Paper No. 05-17, available at http://ssrn.com/abstract=716862 [last check, Jun.5, 2010].

[8] Solove, D. J., (2002), *Conceptualizing Privacy*, California Law Review, 90, 1087, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103 [last check, Jun.5, 2010]. Even in the E.U. legal environment for personal and sensitive data protection, privacy may have different flavours such as the right to be let alone, the right to shield oneself from unwanted access by others, the right for concealment of certain matters from others, the right to control over personal information, and the right to protect one's personality, individuality, and dignity. See, also, Jones, H., and Soltren, J.H., (2005), *Facebook: Threats to privacy*, Project MAC: MIT Project on Mathematics and Computing. For the meaning of Privacy in the E.U. legal framework, see also, the European Court of Human Rights case *Botta v. Italy (153/1996/772/973) February 24, 1998*, available at http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=696017&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166 [last check, Jun.5, 2010], the European Court of Human Rights case *Gaskin v. United Kingdom (10454/83) July 7, 1989*, available at http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=695368&portal=hbkm&source=externalbydocnumber [last check, Jun.5, 2010]; the European Court of Human Rights case *Guerra and Others v Italy (116/1996/735/932) February 19, 1998*, available at http://www.iidh.ed.cr/comunidades/libertadexpresion/docs/le_europeo/guerra%20and%20others%20v.%20italy.htm [last check, Jun.5, 2010]; see also, Mitrou, L., (2010), ibid.

[9] By May 2010, Facebook has become a community of more than 400 million users—almost 500 users. See Zuckerberg, M., (2010), *From Facebook, answering privacy concerns with new settings*, Wall Street Journal, May 24, 2010, available at http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html [last check, Jun.5, 2010]; Fletcher, D., (2010), *Facebook Society—Friends Without Borders*, Time magazine, May 31, 2010, p.18-24, cover page of Time magazine issue of May 31, 2010, under the title *Facebook …and how it's redefining privacy,* available at http://www.time.com/time/business/article/0,8599,1990582,00.html [last check, Jun.5, 2010], according to which within the next few weeks (of June-July 2010), Facebook will officially log its 500 millionth active citizen. *If the website were granted terra firma, it would be the world's third largest country by population, two-thirds bigger than the U.S. More than 1 in 4 people who browse the Internet not only have a Facebook account but have returned to the site within the past 30 days.*

[10] Except Facebook, other social networking sites include ARTO (http://www.arto.com [last check, Jun.5, 2010]), BEBO (http://www.bebo.com [last check, Jun.5, 2010]), DAILYMOTION (http://www.dailymotion.com/gr [last check, Jun.5, 2010]), GIOVANI.IT (http://www.giovani.it [last check, Jun.5, 2010]), HYVES.NL (http://www.hyves.nl [last check, Jun.5, 2010]), MYSPACE (http://www.myspace.com [last check, Jun.5, 2010]), NASZA-KLASA.PL (http://nasza-klasa.pl [last check, Jun.5, 2010]), NETLOG (http://www.netlog.com [last check, Jun.5, 2010]), ONE.LT (http://w29.one.lt/welcome [last check, Jun.5, 2010]), PICZO (http://www.piczo.com/?cr=3 [last check, Jun.5, 2010]), RATE.EE (http://www.rate.ee [last check, Jun.5, 2010]), SKYROCK.COM (http://www.skyrock.com [last check, Jun.5, 2010]), SULAKE (http://www.sulake.com [last check, Jun.5, 2010]), TUENTI (http://www.tuenti.com/?m=login [last check, Jun.5, 2010]), VZNET NETZWERKE LTD. (http://www.meinvz.net/Default [last check, Jun.5, 2010]), , ZAP.LU (http://www.zap.lu [last check, Jun.5, 2010]).

[11] danah michele boyd, a social media researcher and fellow at Harvard University's Berkman Center for Internet and Society has preference in writing and using her name

without any capitalization of her name. Her decision to leave capitalization out of her name is respected, thus any references hereto to her name in consideration of citation to her work will leave capitalization out. See more about her preference regarding writing her name at http://www.danah.org/name.html [last check, Jun.5, 2010].

[12] boyd, d., and Ellison, N., (2007), *Social Networking Sites: Definition, History, and Scholarship*, Journal of Computer-Mediated Communication, 13(1), available at http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html [last check, Jun.5, 2010].

[13] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data,* WP 136/01248/07/EN, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf [last check, Jun.5, 2010].

[14] ENISA Position Paper No.1, (2007), *Security Issues and Recommendations for Online Social Networks*, ed. Giles Hogben, available at http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks [last check, Jun.5, 2010].

[15] Hull G., Lipford H. R., Latulipe C., (2009), ibid.; West, A., Lewis, J., and Currie, P., (2009), *Students' Facebook 'friends': public and private spheres*, Journal of Youth Studies, 12(6), 615-627; Zhao, S., Grasmuck, S., and Martin, J., (2008), *Identity construction on Facebook: Digital empowerment in anchored relationships,* Computers in Human Behavior, 24(5), 1816-1836.

[16] boyd, d., (2008), Taken *out of context: American teen sociality in networked publics*, University of California at Berkeley, available at http://www.danah.org/papers/TakenOutOfContext.pdf [last check, Jun.5, 2010]; Marwick, A., Diaz, D. M., and Palfrey, J., (2010), *Youth, Privacy and Reputation*, Research Publication 2010-5, The Berkman Center for Internet and Society at Harvard University, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163 [last check, Jun.5, 2010].

[17] Facebook Statement of Rights and Responsibilities, 4.Registration and Account Security, available at http://www.facebook.com/#!/terms.php?ref=pf [last check, Jun.5, 2010]. The online collection of personal information from children under 13 years old by persons or entities under the U.S. jurisdiction is illegal according to Children's Online Privacy Protection Act (COPPA) of October 1998, 15 U.S.C. §§ 6501–6506 (2006). Companies operating websites that fall outside COPPA's jurisdiction but still target young people remain under the watch of the Federal Trade Commission (FTC), which has the authority to enforce the commitments made to Internet users under privacy policies under the FTC's general unfair and deceptive practices powers. Since 1998, the FTC has maintained the position that the use or dissemination of personal information in a manner contrary to a posted privacy policy is a deceptive practice under the FTC Act Section 45(a)(1).

[18] Gross, E.F., (2004), *Adolescent Internet use: What we expect, what teens report*, Journal of Applied Developmental Psychology, 25(6), 633-649. According to this study, about half of the 175 7th and 10th graders in her survey had pretended to be someone else online, but of that, almost all had pretended to be older. See, also, Steeves, V., and Webster, C., (2008), *Closing the barn door: the effect of parental supervision on Canadian children's online privacy*, Bulletin of Science, Technology and Society, 28(1), 4-19, who report that the majority (59%) of their 3,000 respondents had, at one time, pretended to be a different age (52%), a different personality (26%), or someone with a different physical appearance (23%). Respondents said they did this for a variety of reasons, including seeing what it would be like, to flirt, to pretend to be older, or to act "mean." More research findings at Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid.

[19] Lwin, M.O., Stanaland, A.J., and Miyazaki, A.D., (2008), *Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness*, Journal of Retailing 84(2), 205-217.

[20] Online fights using electronic messages with angry and vulgar language.

[21] Setting up accounts pretending to be people in order to humiliate them; sending or posting gossip or rumors about a person to damage his or her reputation or friendships.

[22] Pretending to be someone else and sending or posting material to get that person in trouble, and put them in danger or to damage their reputation or friendships.

[23] Sharing someone's secrets or embarrassing information or images online.

[24] Talking someone with the aim to make her into revealing secrets or embarrassing information, and then sharing it online.

[25] Intentionally and cruelly excluding someone from an online group as a form of punishment.

[26] Typically linked to a problematic intimate relationship, repeated, intense harassment and denigration that includes threats or creates significant fear.

[27] ENISA Position Paper No.1, (2007), ibid.

[28] Ito, M., Horst, H., Bittanti. M., boyd D., Herr-Stephenson, B., Lange, P., Pascoe, C., and Robinson L., (2008), *Living and Learning with New Media: Summary of Findings from the Digital Youth Project*, The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning, 52, available at http://www.macfound.org/atf/cf/%7BB0386CE3-8B29-4162-8098-E466FB856794%7D/DML_ETHNOG_WHITEPAPER.PDF [last check, Jun.5, 2010].

[29] Steeves, V., and Webster, C., (2008), ibid. There are research findings, though, that reach different conclusions regarding privacy-protective behavior. Two-large scale studies concluded that slightly less than half of users set their social network profile to private, making it inaccessible to anyone outside their group of friends. See more at Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid.; Hinduja, S., and Patchin, J.W., (2008), *Personal Information of adolescents on the Internet: A quantitative content analysis of MySpace,* Journal of adolescence, 31(1), 125-146; Lenhart, A., and Madden, M., (2007), *Teens, Privacy and Online Social Networks*, Washington DC: Pew Internet and American Life Project, available at http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Privacy_SNS_Report_Final.pdf.pdf [last check, Jun.5, 2010].

[30] Valkenburg, P.M., and Peter, J., (2008), *Adolescents' identity experiments on the Internet: Consequences for social competence and self-concept unity*, Communication Research, 35(2), 208; Govani, T., and Pashley, H., (2007), *Student awareness of the privacy implications when using Facebook,* Carnegie Mellon University, available at http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf [last check, Jun.5, 2010]. See, also, Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid. for further references to related research findings; Tuunaimen, V.K., Pitkanen, O., and Hovi, M., (2009), *Users' Awareness of Privacy on Online Social Networking sites—Case Facebook,* 22nd Bled eConference eEnablement: Facilitating an Open, Effective and Representative eSoceity, available at http://ecom.fov.uni-mb.si/proceedings.nsf/0/9b675b5e811394f0c125760000390664/$FILE/1_Tuunainen.pdf [last check, Jun.5, 2010]. But, more recent reports find that privacy-protecting activities have become considerably more common across all age groups than they were when similar studies were conducted in the past. For example, see Madden, M.,

and Smith, A., (2010), *Reputation Management and Social Media, How People monitor their identity and search for others online,* May 26, 2010, Pew Internet & American Life Project, available at http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management.pdf [last check, Jun.5, 2010] which indicates that a relative lack of concern about the availability of personal information online does not necessarily translate into inaction. Indeed, many of the least concerned Internet users have still taken steps to restrict what they share with others. For example, two-thirds of all social networking users (65%) say they have changed the privacy settings for their profile to limit what they share with others online. Among social networking users who worry about the availability of their online information, fully 77% have changed their privacy settings. However, even those who don't worry about such information are relatively active in this regard—59% of these less concerned social networking users have adjusted their privacy settings in this way.

[31] Livingstone, S., (2005), *Mediating the public/private boundary at home*, Journal of Media Practice, 6(1), 11-151; Steeves, V., and Webster, C., (2008), ibid.; Levin, A., and Abril, P.S., (2009), *Two Notions of Privacy Online*, Vanderbilt Journal of Entertainment and Technology Law, v.11, 1001-1051, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1428422 [last check, Jun.5, 2010].

[32] Aidman, A., (2000), *Children's Online Privacy—What you Need to Know about the Children Online Privacy Protection Act,* Educational Leadership 58(2), 46-48; Giffen, M., (2008), *Online Privacy*, Current Health, 34(7), 8-11; Palfrey, J., Gasser, U., (2008), *Born Digital: Understanding the First Generation of Digital Natives,* New York Basic Books; Palfrey, J., Sacco, D., boyd, d., (2008), *Enhancing Child Safety and Online Technologies: Research Advisory Board Report for the Internet Safety Technical task Force*, Cambridge MA: The Berkman Center for Internet and Society at Harvard University; Youn, S., (2009), *Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents*, Journal of Consumer Affairs, 43(3), 389-418; Lenhart, A., and Madden, M., (2007), ibid.

[33] Grimmelmann, J., (2009), *Saving Facebook*, Iowa Law Review, 94 (1137).

[34] Hull G., Lipford H. R., Latulipe C., (2009), ibid.

[35] Christofides, E., Muise, A., and Desmarais, S., (2009), *Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?*, CyberPsychology & Behavior, 12(3), 341-345; Debatin, B., Lovejoy, J., Horn, A.K., and Hughes, B., (2009), *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences*, Journal of Computer-Mediated Communication, 15(1), 83-108.

[36] Weibel, P., (2002), *Pleasure and the Panoptic Principle*, CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother, ed. Thomas Y. Lenin et. al. Cambridge MA MIT Press, 206-223.

[37] Gross, R., and Acquisti, A., (2005), *Information Revelation and Privacy in Online Social Networks (The Facebook case)*, ACM Workshop in Privacy in the Electronic Society (WPES).

[38] Christofides, E., Muise, A., and Desmarais, S., (2009), ibid.

[39] See, for example, how respected blogger Will McInnes explains Facebook users' stance regarding their privacy through Facebook, in Brown, B., (2009), *Net guru on Facebook data policy*, video BBC News, February 18, 2009, available at http://news.bbc.co.uk/2/hi/technology/7897824.stm [last check, Jun.5, 2010].

[40] West, A., Lewis, J., and Currie, P., (2009), ibid.

[41] Studies of identity construction on Facebook have found that people construct strategic identities that reflect their social wannabes. See Liu, H., (2007), *Social network profiles as taste performances*, Journal of Computer-Mediated Communication, 13(1), 252; Zhao, S., Grasmuck, S., and Martin, J., (2008), ibid.

[42] Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid. refer to this publicity quest as 'micro-celebrity' identity construction that is presented to one's audience in Facebook and is most likely constructed with the audience in mind, emphasizing qualities considered high-status within that community and de-emphasizing attributes that are not characteristic of the publicity-seeker's environment.

[43] That explains why people who leverage on publicity with the aim to make profit tend to flock in Facebook and other social networking media, daily. There are many examples for this tendency of professionals such as lawyers, especially young ones with an insentient thirst to become known, who post onto Facebook any kind of information, relevant or irrelevant, to their professional activities, stupid or not, aiming at attracting the eyeballs of any Facebook user who could support their self-publicity cause. Research indicates that the use of social network sites, which require the sharing of personal information, allows young people to maintain weak ties, strengthen friendships, increase social capital, and gain popularity (e.g. see Ellison, N., Steinfield, C., and Lampe, C., (2007), *The Benefits of Facebook 'friends': social capital and college students' use of online social network sites*, Journal of Computer-Mediated Communication, 12(4), 1143; Joinson, A.N., (2008), *Looking at, looking up or keeping up with people?: motives and use of Facebook*, CHI Proceedings—Online Social Networks). This publicity quest of young professionals reminds me Oscar Wild's cynical saying "*The only thing worse than being talked about is not being talked about*." Yet, aside from this consideration, the posting onto Facebook of any nook and cranny of a lawyer's life, especially of information pertaining to his/her professional life and clients, is of questionable legality, especially in relation to Lawyer's Code of Conduct, i.e. Law 3026/1954 for Lawyers in Greece as it stands now—one could predict that said law will soon be amended so that lawyers are allowed to advertise themselves, but no amendment is predicted regarding a lawyer's obligation not to reveal to any third party matters upon his/her clientele. Said public speaking upon a lawyer's professional life through Facebook is, also, profoundly stupid, provocative, and indicative of a lack of professionalism as well as lack of any sense of privacy protection. For one thing if Facebook is clear currently is the fact that information posted onto its Platform will become public. And once said information is public none can tell how this information will be handled and used by any third party. The inability to tell how information provided online will be handled and used is referred to as "information risk". Though studies repeatedly have shown that "information risk" increases concerns over privacy when users do not know how their personal information will be used (e.g. see Youn, S., (2009), ibid.; Sheehan, K.B., and Hoy, M.G., (1999), *Flaming, complaining, abstaining: How online users respond to privacy concerns*, Journal of Advertising, 28(3), 37-51), and though that increased "information risk" increases the likelihood of a person adopting privacy-protecting behaviors, yet lawyers who do exactly the opposite by posting every aspect of their (professional) life onto Facebook with the aim to become known and be talked about do nothing more than bluntly self-advertise in a rather stupid and amateurish way and self-promote either ignorance and naivety or disrespect in terms of data protection, at least. On the other hand, decisions taken by Bar Associations such as the Athens Bar Association's decision of May 20, 2009, (see the decision at http://www.dsa.gr/index.phtml?url=news&categ=%CD%DD%E1-%C1%ED%E1%EA%EF%E9%ED%FE%F3%E5%E9%F2&id=417113&search=yes&searchkeywords=Internet [last check, Jun.5, 2010]) with the aim to restrict lawyers' use of the Internet do not make any sense because 1) said decisions can hardly be imposed on the Bar Association's members; 2) said decisions are wrong to the point that they consider the Internet as merely an advertising medium; the Internet and Internet applications are much more than that; 3) though said decisions consider

lawyers' online behavior which might be in conflict with Lawyer's Code of Conduct which currently forbids lawyers' advertising, yet, in most cases, criticized lawyers' behavior online might not be an issue of direct and/or indirect advertising or any other issue of professional standards in accordance with current legislation, but rather it might be a matter of lack of common sense as well as bad aesthetics in their presence online; while Bar Associations are organizations appropriate to instruct on professional standards, yet they are not appropriate to command on common sense and aesthetics.

[44] ChoicePoint, one of the largest data brokers in the world, in early 2005 admitted that it had released sensitive data on roughly 163,000 people to fraudsters who signed up as ChoicePoint customers starting in 2001. At least 800 cases of identity theft resulted. Sued by the FTC, the company paid USD $15 million in a settlement by 2006, at least USD $5 million of which went to the consumers whose lives they ruined. See more at http://www.wired.com/politics/security/news/2006/08/71622#ixzz0oNuTAjQx [last check, Jun.5, 2010]; in February 2008, ChoicePoint was purchased by Reed Elsevier for 3.6 billion USD $. See more about ChoicePoint at Wikipedia at http://en.wikipedia.org/wiki/ChoicePoint [last check, Jun.5, 2010].

[45] Digital dossiers of personal information may result in cases of discrimination against individuals based on their personal data or in cases of identity theft, stalking, harassment, and other invasions of privacy. See more at Ciocchetti, C., (2007), *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, American Business Law Journal 44(1), 55-126; Palfrey, J., and Gasser, U., (2008), ibid.; ENISA Position Paper No.1, (2007), ibid.

[46] Solove, D., (2004), *The Digital Person: Technology and privacy in the information age,* New York University Press.

[47] Xie, E., Teo, H., and Wan, W., (2006), *Volunteering personal information on the Internet: Effects of reputation, privacy notices, and rewards on online consumer behavior*, Marketing Letters, 17(1), 61-74; Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid.; Hendry, J., and Goodall, K., (2010), *Facebook and the Commercialisation of Personal Information: Some Questions of Provider-to-User Privacy*, in M.E.A. Goodwin, B.J. Koops and R.E. Leenes, eds., Dimensions of Technology Regulation, Wolf Legal Publishing.

[48] Peterson, C., (2010), *Losing Face: an Environmental Analysis of Privacy on Facebook*, available at http://etc.cpeterson.org/research/workingpapers/2010/losingface_workingpaper.pdf [last check, Jun.5, 2010].

[49] Face-recognition technology is used with the aim to identify a Facebook user who though she posts—or any third party posts—online a photograph of herself, she uses pseudo-anonymous profile. See ENISA Position Paper No.1, (2007), ibid.

[50] Content-based Image Retrieval (CBIR) is an emerging technology which can match features, such as identifying aspects of a room (e.g. a painting) in very large databases, increasing the possibilities for locating users. See ENISA Position Paper No.1, (2007), ibid.

[51] Many SNSs now allow users to tag images with metadata, such as links to SNS profiles (even if they are not the owner/controller of that profile), or even e-mail addresses. This leads to greater possibilities for unwanted linkage to personal data. See ENISA Position Paper No.1, (2007), ibid.

[52] Unsolicited messages propagated using SNSs. See ENISA Position Paper No.1, (2007), ibid.

[53] SNSs are vulnerable to XSS attacks and threats due to 'widgets' produced by weakly verified third parties. See ENISA Position Paper No.1, (2007), ibid.

[54] 'SNS portals' integrate several SNSs which multiply vulnerabilities by giving read/write access to several SNS accounts using a single weak authentication. See ENISA Position Paper No.1, (2007), ibid.

[55] Cyber-stalking is threatening behavior in which a perpetrator repeatedly contacts a victim by electronic means such as email, Instant Messenger and messaging on SNSs. Statistics suggest that stalking using SNSs is increasing. ENISA Position Paper No.1, (2007), ibid.

[56] Cyber-bullying is the behavior of repeated and purposeful acts of harm such as harassment, humiliation and secret sharing. ENISA Position Paper No.1, (2007), ibid.

[57] Solove, D., (2004), ibid. He speaks for a 'Kafkaesque world of bureaucracy' where people are vulnerable to exploitation of their personal information and subject to a bureaucratic process that is itself not adequately controlled. See, also, Palfrey, J., Gasser, U., (2008), ibid.

[58] Data Protection and Freedom of Information Commissioner of the State of Berlin, Germany, (2008), *Resolution on Privacy Protection in Social Network Services*, available at http://www.lda.brandenburg.de/sixcms/media.php/3509/resolution_social_networks_en.pdf [last check, Jun.5, 2010].

[59] Hull G., Lipford H. R., Latulipe C., (2009), ibid.

[60] boyed, d., (2007), *Why Youth (Heart) Social Network Sites: The Role of Networked Publics*, in D. Buckingham , ed. Youth Identity and Digital Media, Cambridge MA: MIT Press.

[61] Benkler, Y., (2006), *The Wealth of Networks: How Social Production transforms Markets and Freedom*, Yale University Press, Chapter 10: Social Ties: Networking Together, available at http://cyber.law.harvard.edu/wealth_of_networks/Main_Page [last check, Jun.5, 2010].

[62] Benkler, Y., (2006), ibid.

[63] Jones, H., and Soltren, J.H., (2005), ibid.

[64] Govani, T., and Pashley, H., (2007), ibid.

[65] Hull G., Lipford H. R., Latulipe C., (2009), ibid.

[66] Strater K., and Lipford H.R., (2008), *Strategies and Struggles with Privacy in Online Social Networking Community*, Proceedings of the 22nd British HCI Group, ACM Press, p.111-119. Solove D., (2007), *The Future of Reputation: Gossip, Rumor and Privacy on the Internet*, New Haven, Yale University Press.

[67] Hashemi Y., (2009), *Facebook's privacy policy and its third-party partnerships: lucrativity and liability*, Boston University Journal of Science and Technology Law 15, 140-61.

[68] Facebook statistics on the use of its Platform and Platform applications, available at http://www.facebook.com/press/info.php?factsheet#!/press/info.php?statistics [last check, Jun.5, 2010].

[69] Goettke, R., and Christiana, J., (2007), *Privacy and Online Social Networking Websites*; Nissenbaum, H., (2004), ibid.

[70] boyd, d., (2008), *Facebook's Privacy Trainwreck – Exposure, Invasion, and Social Convergence*, available at http://www.danah.org/papers/FacebookPrivacyTrainwreck.pdf [last check, Jun.5, 2010].

[71] Facebook Privacy Policy, How We Share Information states that "*Facebook is about sharing information with others — friends and people in your communities — while providing you with privacy settings that you can use to restrict other users from accessing some of your information. We share your information with third parties when we believe the sharing is permitted by you, reasonably necessary to offer our services, or when legally required to do so.*" Facebook may be seen as a 'digital cocktail party'. In general, the more contacts you have, the more popular you are, and the more influence you have. However, compared with real-world cocktail parties, Facebook members broadcast information much more widely, either by choice or by mistake. See ENISA Position Paper No.1, (2007), ibid.

[72] Picker, R., (2009), *Online Advertising, Identity and Privacy*, The Law School, The University of Chicago Law and Economics, working paper No. 475, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1428065 [last check, Jun.5, 2010].

[73] Opsahl, K., (2010), *Facebook's Eroding Privacy Policy: A Timeline*, Electronic Frontier Foundation, Deeplinks Blog, available at http://www.eff.org/deeplinks/2010/04/facebook-timeline [last check, Jun.5, 2010].

[74] Opsahl, K., (2010), ibid.

[75] See Article 29 Data Protection Working Party, *European data protection group faults Facebook for privacy setting change*, Press Release of May 12, 2010, available at http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_12_05_10_en.pdf [last check, Jun.5, 2010].

[76] The Fourth Amendment protection posits that an individual has an expectation of privacy where (1) the individual possesses a subjective expectation of privacy; and (2) that expectation is "one that society is prepared to recognize as "reasonable". The opinion of the Supreme Court of the U.S. in the case Katz v. United States, 389 U.S. 347 (1967) available at http://supreme.justia.com/us/389/347/case.html [last check, Jun.5, 2010] is that "*What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.* See Lewis v. United States, *385 U. S. 206, 385 U. S. 210;* United States v. Lee, *274 U. S. 559, 274 U. S. 563. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected*."

[77] This is the case of what D. Solove refers to as the "secrecy paradigm." See Solove, D., (2004), ibid.

[78] Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid.

[79] For the "third-party doctrine" see Solove, D., (2005), *A Taxonomy of Privacy*, University of Pennsylvania Law Review, 154(3), 477; Palfrey, J., (2008), *The Public and the Private at the United States Border with Cyberspace*, Mississippi Law Journal 78, 241-294; Kerr, O.S., (2009), *The Case for the Third-Party Doctrine*, Michigan Law Review 107(561), 561-602, available at http://www.michiganlawreview.org/assets/pdfs/107/4/kerr.pdf [last check, Jun.5, 2010]; the same, (2009), *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, Berkeley Technology Law Journal 24, 1229-1236, available through

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1608013 [last check, Jun.5, 2010]; Epstein, R.A., (2009), *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, Berkeley Technology Law Journal 24(3), 1199.

[80] Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid.

[81] According to the FOIA (See FOIA through the http://www.justice.gov/oip [last check, Jun.5, 2010]), federal agencies of the U.S. Government generally are required to disclose records requested in writing by any person. The FOIA applies only to federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies. Each State in the U.S. has its own public access laws that should be consulted for access to state and local records.

[82] On December 1, 2009, the Electronic Frontier Foundation submitted a complaint for injunctive relief in the U.S. District Court for the Northern District of California, San Francisco Division, against the Department of Defense (DoD), the Central Intelligence Agency (CIA), the Department of Homeland Security (DHS), the Department of Justice (DoJ), the Department of Treasury (DoT), and the Office of the Director of National Intelligence (ODNI) of the U.S. Government, claiming the Plaintiff that the Defendants do not have any legal ground in consideration of FOIA, 5 U.S.C. § 552 for their investigative, surveillance and data-mining practices through social networking sites such as Facebook and MySpace (See the Complaint at http://www.eff.org/files/filenode/social_network/social_networking_FOIA_complaint_final.pdf [last check, Jun.5, 2010]). The reply to the requested injunctive relief was issued on February 8, 2010 (See the Answer to the Complaint at http://www.eff.org/files/filenode/social_network/social_networking_FOIA_answer_0.pdf [last check, Jun.5, 2010]), in which almost all Defendants answered that they lack sufficient knowledge or information to admit or deny the allegations of the Plaintiff, i.e. they claim that they do not know whether data-mining for investigative, surveillance or any other purposes is happening. The Court, also, ruled that Defendants rightfully asserted that Plaintiff was not entitled to the relief requested, or to any relief whatsoever, and ruled that Plaintiff's action be dismissed in its entirety with prejudice and that Defendants be given such other relief as the Court deemed proper, including costs and disbursements. See, also, Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid. regarding the 2009 action taken by The New York Times against the U.S. Government based on the FOIA with the request for the extent of law enforcement requests for social media site information. Also, *Complaint* against Facebook Inc. has been submitted to the U.S. Federal Trade Commission by the Electronic Privacy Information Center (EPIC), on December 17, 2009 (see the *Complaint* at http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf [last check, Jun.5, 2010]; and *supplemental materials to the Complaint* at http://epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf [last check, Jun.5, 2010]); and a second *Complaint, Investigation request and Injunction and Other relief* submitted to FTC on May 10, 2010, by EPIC and 14 privacy and consumer protection organizations in the U.S., i.e. The Bill of Rights Defense Committee, The Center for Digital Democracy, The Center for Financial Privacy and Human Rights, Center for Media and Democracy, Consumer Federation of America, Consumer Task Force for Automotive Issues, Consumer Watchdog, FoolProof Financial Education, Patient Privacy Rights, Privacy Activism, Privacy Journal, The Privacy Rights Clearinghouse, The U.S. Bill of Rights Foundation, U.S. PIRG, available at http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf [last check, Jun.5, 2010]. EPIC's second complaint is charging that Facebook has engaged in unfair and deceptive trade practices in violation of consumer protection law. The complaint states that changes to user profile information and the disclosure of user data to third parties without consent "violate user expectations, diminish user privacy, and contradict Facebook's own representations." The complaint also cites widespread opposition from Facebook users, Senators (see April 27, 2010 letter of Senators Charles E. Schumer, Michael F. Bennet, Mark Begich, and Al Franken to Mark Zuckerberg available at http://voices.washingtonpost.com/posttech/Schumer-Franken-Bennet-

Begich%20Letter%20to%20Facebook%204.27.10.pdf [last check, Jun.5, 2010]), bloggers, and news organizations. In a letter to Congress (see it at http://epic.org/privacy/facebook/EPIC_FB_FTC_Complaint_Letter.pdf [last check, Jun.5, 2010]), EPIC urged the Senate and House Committees with jurisdiction over the FTC to monitor closely the Commission's investigation. The letter noted the FTC's failure to act on several pending consumer privacy complaints.

[83] On March 16, 2010, the EFF posted online documents shedding light on how U.S. law enforcement agencies use social networking sites to gather information in investigations. The records, obtained from the Internal Revenue Service and Department of Justice Criminal Division. The U.S. IRS employees are trained through a 2009 training course with the aim to use various Internet tools—including social networking sites and Google Street View—in order to investigate taxpayers. The U.S. Department of Justice Computer Crime and Intellectual Property Section were found to present detail information upon several social media companies' data retention practices and responses to law enforcement requests. Facebook was reported in said information to be "often cooperative with emergency requests" from said agencies. See more, Hofmann, M., (2010), *EFF Posts Documents Detailing Law Enforcement Collection of Data From Social Media Sites*, available at http://www.eff.org/deeplinks/2010/03/eff-posts-documents-detailing-law-enforcement [last check, Jun.5, 2010].

[84] Marwick, A., Diaz, D. M., and Palfrey, J., (010), ibid.

[85] One example of secondary uses that has gained wide public attention is the practice of company personnel managers crawling user profiles of job applicants or employees: According to press reports, one third of human resources managers already admit to use data from social network services in their work, e.g. to verify and/or complete details of job applicants. See, also, related video titled *Facebook Killed the Private Life*, November 6, 2007, and discussion with Clay Shirky, Professor at New York University, expert on new media and social network media, available at http://www.youtube.com/watch?feature=related&hl=el&v=azIW1xjSTCo [last check, Jun.5, 2010].

[86] Marwick, A., Diaz, D. M., and Palfrey, J., (2010), ibid.; Debatin, B., Lovejoy, J., Horn, A.K., and Hughes, B., (2009), ibid.; Jones, H., and Soltren, J.H., (2005), ibid.

[87] Iglezakis, I., (2010), *Privacy Protection and Electronic Governance*, in Protection of Privacy & Information and Communication Technologies—Technical and Legal issues, Labrinoudakis, K., Mitrou, L., Gritzalis, S., Katsikas, S., eds., Papassotiriou publications; Sotiropoulos, V., (2007), *Further Use of Information in the Public Sector*, Sakkoulas Publications.

[88] RISEPTIS Report, (2009), *Trust in the Information Society*, A Report of the Advisory Board, RISEPTIS (Research and Innovation on Security, Privacy and Trustworthiness in the Information Society), available at http://www.think-trust.eu/general/news-events/riseptis-report.html [last check, Jun.5, 2010].

[89] European Commission, (2010), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, A Digital Agenda for Europe, COM(2010) 245*, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF [last check, Jun.5, 2010].

[90] The European Data Protection Supervisor, (2010), *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, March 18, 2010, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consu

ltation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf [last check, Jun.5, 2010]; European Commission, (2010), COM(2010) 245, ibid.

[91] European Commission, (2010), COM(2010) 245, ibid.

[92] 'Privacy by Design' is introduced as a new principle in the E.U. which is not only relevant for responsible controllers, but also for vendors and developers. It is certain that there will also be some scope for 'Privacy by Default' settings in specific areas such as RFID, social networking sites and cloud computing. See Hustinx, P., (2010), *Making data protection more effective: challenges and opportunities*, ICT Committee - Breakfast Roundtable: "Data Loss Prevention – Is sensitive information leaving your organization?" March 9, 2010, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-03-09_DP_more_effective_EN.pdf [last check, Jun.5, 2010]; the same, (2010), *Recent developments in the European Union*, speech given at Joint ICCP-WPISP Roundtable "30 years after: the impact of the OECD Privacy Guidelines", Paris, March 10, 2010, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-03-10_Privacy_guidelines_EN.pdf [last check, Jun.5, 2010].

[93] Wong, R., (2009), *Social Networking: a conceptual analysis of a data controller*, Communications Law v.14(5) 142, available at http://works.bepress.com/cgi/viewcontent.cgi?article=1008&context=rebecca_wong [last check, Jun.5, 2010]; Article 29 Data Protection Working Party, *Opinion 5/2009 on social networking party*, WP 163/01189/09/EN, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf [last check, Jun.5, 2010].

[94] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169/00264/10/EN, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf [last check, Jun.5, 2010].

[95] When Facebook users do not change privacy settings for any reason including the fact that may be unaware of the implications of not changing them or do not know how to do it, this fact of not changing the privacy settings cannot mean in consideration of data protection law in Europe that individuals have made an informed decision to accept sharing information through Facebook Platform and/or Applications which favor disclosure of personal data by default. See more at The European Data Protection Supervisor, (2010), ibid.

[96] These risks have already been analyzed in the "*Report and Guidance on Privacy in Social Network Services*" (*Rome Memorandum*) of the 43rd meeting of the International Working Group on Data Protection in Telecommunications (3-4 March 2008), and in the ENISA Position Paper No.1 "*Security Issues and Recommendations for Online Social Networks.*"

[97] The European Data Protection Supervisor, (2010), ibid.

[98] Facebook Privacy Policy, Risks inherent in sharing information, available at http://www.facebook.com/policy.php [last check, Jun.5, 2010]: "*Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings.*"

[99] Piskopani, A.M., (2010), *The Facebook Phenomenon: Dismantling Privacy Protection Law*, in Protection of Privacy & Information and Communication

Technologies—Technical and Legal issues, Labrinoudakis, K., Mitrou, L., Gritzalis, S., Katsikas, S., eds., Papassotiriou publications.

[100] Fung P., (2007), *Public Search Listings on Facebook*, Posting to the Facebook Blog on Sept.5, 2007, available at http://blog.facebook.com/blog.php?post=2963412130 [last check, Jun.5, 2010].

[101] Fung P., (2007), ibid. The information that Facebook users posted through Facebook Platform and which went public was information that by default everyone could have access to. It was "Everyone" Information in the sense that information set to everyone "*is publicly available information, just like your name, profile picture, and connections. Such information may, for example, be accessed by everyone on the Internet (including people not logged into Facebook), be indexed by third party search engines, and be imported, exported, distributed, and redistributed by us and others without privacy limitations. Such information may also be associated with you, including your name and profile picture, even outside of Facebook, such as on public search engines and when you visit other sites on the internet. The default privacy setting for certain types of information you post on Facebook is set to "everyone." You can review and change the default settings in your privacy settings. If you delete "everyone" content that you posted on Facebook, we will remove it from your Facebook profile, but have no control over its use outside of Facebook.*"

[102] Abram C., (2007), *Pass it on*, Posting to the Facebook Blog on Dec.18, 2007, available at http://blog.facebook.com/blog.php?post=7830237130 [last check, Jun.5, 2010].

[103] Abram C., (2007), ibid.

[104] Abram C., (2007), ibid.

[105] Facebook Privacy Policy states that "*You can also use your privacy settings to limit which of your information is available to 'everyone'*". Thus, the 'everyone' becomes the default for information posted in Facebook Platform by its users.

[106] The Facebook principles is now expressed through the Facebook Privacy Policy text that is available at http://www.facebook.com/policy.php [last check, Jun.5, 2010].

[107] Hashemi Y., (2009), ibid. The same meaning is now expressed in rephrase through the Facebook Privacy Policy in the Risks inherent in sharing information, which states that "*Although we allow you to set privacy options that limit access to your information, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other users with whom you share your information. We cannot guarantee that only authorized persons will view your information. We cannot ensure that information you share on Facebook will not become publicly available. We are not responsible for third party circumvention of any privacy settings or security measures on Facebook. You can reduce these risks by using common sense security practices such as choosing a strong password, using different passwords for different services, and using up to date antivirus software.*"

[108] Facebook Privacy Policy, Risks inherent in sharing information, available at http://www.facebook.com/policy.php [last check, Jun.5, 2010].

[109] Facebook Privacy Policy reminds—among other issues –to its users that when they post information on another user's profile or comment on another user's post, that information will be subject to the other user's privacy settings. If they use an external source to publish information to Facebook (such as a mobile application or a Connect site), they should check the privacy setting for that post, as it is set by that external source.

[110] Facebook announced its intention to keep copies of users' messages online, even after they had left the network. But this decision was met with severe Facebook users' protests, and Facebook was forced to retreat from implementing this plan. See, Johnson B., and Hirsch A., (2009), *Facebook backtracks after online privacy protests*, available at http://www.guardian.co.uk/technology/2009/feb/19/facebook-personal-data [last check, Jun.5, 2010].

[111] Elkins S., (2007), *A Social Network's Faux Pas?*, Newsweek, available at http://www.newsweek.com/id/69275 [last check, Jun.5, 2010]. See also Facebook groups titled "*Petition: Facebook, stop invading my privacy*" available at http://www.facebook.com/group.php?gid=5930262681 [last check, Jun.5, 2010] that counts more than 72,000 members; and "*Millions Against Facebook's Privacy Policies and Layout Redesign*" available at http://www.facebook.com/group.php?gid=27233634858 [last check, Jun.5, 2010] that counts more than 2,273,000 members; and "*News feed Was the Least of our Worries—People Against an Open Facebook*" available at http://www.facebook.com/group.php?gid=2210053630 [last check, Jun.5, 2010].

[112] Hashemi Y., (2009), ibid., describes very low response from Facebook users to relevant Facebook groups protesting about public search listings.

[113] McGeveran, W., (2007), *Facebook Inserting Users Into Ads*, post in Info/Law Blog available at http://blogs.law.harvard.edu/infolaw/2007/11/08/facebook-social-ads [last check, Jun.5, 2010].

[114] McCarthy, C., (2007), *Legally, Are Facebook Social Ads Kosher?*, C|Net News, available at http://news.cnet.com/8301-13577_3-9817421-36.html [last check, Jun.5, 2010].

[115] Felt, A., and Evans, D., (2008), *Privacy Protection for Social Networking APIs*, available at http://www.eecs.berkeley.edu/~afelt/privacybyproxy.pdf [last check, Jun.5, 2010]; Felt, A., (2007), *Defacing Facebook: A Security Case Study*, available at http://www.eecs.berkeley.edu/~afelt/facebook-xss.pdf [last check, Jun.5, 2010].

[116] Facebook Privacy Policy includes clauses regarding information sharing and third parties in which Facebook states that "*We do not own or operate the applications or websites that you use through Facebook Platform (such as games and utilities). Whenever you connect with a Platform application or website, we will receive information from them, including information about actions you take. In some cases, in order to personalize the process of connecting, we may receive a limited amount of information even before you connect with the application or website.*" Facebook also warns a user that "*You should always review the policies of third party applications and websites to make sure you are comfortable with the ways in which they use information you share with them. We do not guarantee that they will follow our rules. If you find an application or website that violates our rules, you should report the violation to us on this help page and we will take action as necessary.*"

[117] Piskopani, A.M., (2009), *Privacy Protection for Facebook users*, DiMEE magazine, 3/2009, v.23, 338-353; the same, (2010), ibid.

[118] Facebook Privacy Policy, Information You Share with Third parties also states that "*When you connect with an application or website it will have access to General Information about you. The term General Information includes your and your friends' names, profile pictures, gender, user IDs, connections, and any content shared using the Everyone privacy setting. We may also make information about the location of your computer or access device and your age available to applications and websites in order to help them implement appropriate security measures and control the distribution of age-appropriate content. If the application or website wants to access any other data, it will have to ask for your permission.*"

[119] Hull G., Lipford H. R., Latulipe C., (2009), *Contextual Gaps: Privacy Issues on Facebook*.

[120] Hull G., Lipford H. R., Latulipe C., (2009), ibid.

[121] In a recent experiment, antivirus company Sophos created a profile page for 'Freddi Staur' (an anagram of 'ID Fraudster'), a green plastic frog with only minimal personal information in his profile. They then sent out 200 friend requests to see how many people would respond, and how much personal information could be gleaned from the respondents. The following are some of the results: a) 87 of the 200 users contacted responded to Freddi, with 82 leaking personal information (41% of those approached); b) 72% of respondents divulged one or more email address; c) 84% of respondents listed their full date of birth. See more Sophos, (2007), *Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves*, available at www.sophos.com/pressoffice/news/articles/2007/08/facebook.html [last check, Jun.5, 2010].

[122] Google's cache and the Internet Archive's Wayback Machine can be used with the aim to retrieve the online tracks which people leave.

[123] Hull G., Lipford H. R., Latulipe C., (2009), ibid. And even when she deletes them, it cannot be taken for granted that the deleted content is not traceable and visible at all.

[124] Hull G., Lipford H. R., Latulipe C., (2009), ibid.

[125] Pearlman, L., (2007), *Facebook Ads*, Posting to the Facebook Blog on Nov.7, 2007, available at http://blog.facebook.com/blog.php?post=6972252130 [last check, Jun.5, 2010].

[126] Facebook Privacy Policy describes social advertising through Facebook Platform as a pairing of relevant information that Facebook has about the user and her friends' behavior through the Platform with the aim to make advertisements more interesting and more tailored to the user and her friends. For example, Facebook states that if a user connects with her favorite band's page, Facebook may display her name and profile photo next to an advertisement for that page that is displayed to her friends.

[127] In Facebook Privacy Policy, Facebook states that they share the personally identifiable information visible in the social ad only with the user's friend who can see the ad. Users can opt out of having their information used in social ads.

[128] Hashemi Y., (2009), ibid.

[129] Traditionally the number of visitors of a website is used as a measure of this website's success. Conversion tracking is a process to find out how many of these visitors perform actions on this website that the website operators and/or right-holders want them to perform. Any marketing campaign is pretty useless if it generates many visitors of a website but none of these visitors is "converted" into a customer. Converting visitors to customers is what most of todays commercial websites are about. Conversion Tracking is a form of website traffic analytics that measures the effectiveness of a source directing visitors to a website and persuading them to take a desired action. The source could be a referrer, a search engine, a search phrase used etc. It could also be a characteristic of the visitor for instance the country, age, income, or any other data—including personal or sensitive data—about the data subject. The desired action could be the completion of an order page, the sign-up of a newsletter, service etc offered in or through the commercial website. The effectiveness is expressed as a percentage called the "conversion rate."

[130] There are many conversion tracking methods such as the *Log Analysis* method according to which the log files generated by the web server on which a website resides are analyzed. Conversion tracking reports are generated which are used for analysis. There is also the *Tracking Services* method according to which tracking script is inserted into pages of the website to be tracked. Page requests from visitors triggers the tracking script which updates some kind of a database at the tracking service. Authorized personnel log into the tracking service and generate reports which are used for analysis. There are other methods for conversion tracking, too.

[131] Facebook does not provide any clarifications or examples upon the non-personally identifiable attributes of its users. It does not, also, provide any clarifications upon the anonymization process that the company follows with the aim to covert personal and sensitive data to non-personally identifiable attributes.

[132] Facebook Privacy Policy, To serve personalized advertising to you, states that "*We don't share your information with advertisers without your consent. (An example of consent would be if you asked us to provide your shipping address to an advertiser to receive a free sample.) We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show to other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements.*"

[133] Hotaling, A., (2008), Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting, CommLaw Conspectus, v.16 (2008), 529-565, available at http://commlaw.cua.edu/res/docs/11_Hotaling.pdf [last check, Jun.5, 2010].

[134] See video titled *Mike Arrington interrogates Mark Zuckerberg*, Upstream Recorded Live, January 8, 2010, available at http://www.ustream.tv/recorded/3848950 [last check, Jun.5, 2010].

[135] Fletcher, D., (2010) ibid., Time magazine, May 31, 2010.

[136] Kirkpatrick, M., (2009), *Zuckerberg Changes His Own Privacy Settings*, December 11, 2009, available at http://www.readwriteweb.com/archives/zuckerberg_changes_his_own_privacy_settings.php [last check, Jun.5, 2010]; the same, (2009), *Why Facebook Changed its Privacy Strategy*, December 10, 2009, available at http://www.readwriteweb.com/archives/why_facebook_changed_privacy_policies.php [last check, Jun.5, 2010]. See, also, video titled *60 Minutes—Facebook*, January 14, 2008, available at http://www.youtube.com/watch?v=1UNrqz6X-AE&feature=related [last check, Jun.5, 2010].

[137] Kirkpatrick, M., (2010), *Mark Zuckerberg on Data Portability: An Interview*, ReadWriteWeb, March 10, 2010, available at http://www.readwriteweb.com/archives/mark_zuckerberg_on_data_portab.php [last check, Jun.5, 2010].

[138] Trevelyan, L., (2009), *Facebook answers critics on privacy*, video BBC News, February 27, 2009, available at http://news.bbc.co.uk/2/hi/business/7916137.stm [last check, Jun.5, 2010].

[139] See, for example, Facebook's retreat regarding the use of people's picture and profile information, in Higham, N., (2009), *Facebook 'withdraws' data changes*, video BBC News, February 18, 2009, available at http://news.bbc.co.uk/2/hi/science/nature/7897172.stm [last check, Jun.5, 2010].

[140] See, for example, Denham, E., (2009), *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,* available at http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf [last check, Jun.5, 2010].

[141] Such as ENISA, Article 29 Data Protection Working Party, European Data Protection Supervisor, to name a few.

[142] The European Commission has entered into an agreement with twenty social network providers known as the "*Safer Social Networking Principles for the EU*," available at http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf [last check, Jun.5, 2010]. See, also, *Report on the assessment of the implementation of the Safer Social Network Principles for the EU*, available at: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf [last check, Jun.5, 2010]. See, also, International Working Group on Data Protection in Telecommunications, (2008), *Report and Guidance on Privacy in Social Network Services—Rome Memorandum*, 43rd meeting, 675.36.5.

[143] Liu, J., (2010), Facebook privacy settings 'unacceptable', video BBC News, May 13, 2010, available at http://news.bbc.co.uk/2/hi/business/8681781.stm [last check, Jun.5, 2010]

[144] Indicatively cited news coverage on Facebook and privacy: IN.GR, (2010), *Quit Facebook Day—After Facebook, what?*, May 25, 2010; see, also, site titled *We Are Quitting Facebook, May 31, 2010*, available at http://www.quitfacebookday.com [last check, Jun.5, 2010], which has been created by Facebook users who protest against the company's alleged lack of respect for users' personal data. By May 31, 2010, the Facebook Quitters leaving Facebook via said site counted to more than 34,000 users; TA NEA, (2010), *Facebook under siege*, May 22, 2010; TO VIMA, (2010), *Protesting for data use -- Disenchanted users organize campaign to sign out Facebook*, May 23, 2010; KATHIMERINI, (2010), *Facebook: Firings from U.S.A. and E.U. regarding personal data*, May 13, 2010; KATHIMERINI, (2010), *Front Against Facebook in Germany because of Personal Data*, April 7, 2010; TA NEA, (2010), *Facebook gave out Instant Messages of its users*, May 6, 2010; Helft, M., (2010), *Facebook Bows to Pressure Over Privacy*, New York Times, May 26, 2010; Worthen, B., (2010), *Facebook Redesigns Privacy Controls*, Wall Street Journal, May 27, 2010; Wortham, J., (2010), *Facebook retools privacy control—Simplified settings unveiled in response to outcry over accessibility of data*, Boston Globe, May 27, 2010; Liedtke, M., (2010), *Senators see privacy problem in Facebook expansion*, Boston Globe, April 27, 2010; Perez, S., (2009), *How Facebook's New Privacy Changes Will Affect You*, ReadWriteWeb, December 2, 2009; Kirkpatrick, M., (2010), *The Facebook Privacy debate: What You Need to Know*, ReadWriteWeb, January 18, 2010; Kirkpatrick, M., (2009), *The Day Has Come: Facebook Pushes People to Go Public*, ReadWriteWeb, December 9, 2009, available at http://www.readwriteweb.com/archives/facebook_pushes_people_to_go_public.php [last check, Jun.5, 2010]; the same, (2009), *Facebook Wants You to Be Less Private—But Why?*, ReadWriteWeb, July 1, 2009; the same, (2009), A Closer Look at Facebook's New Privacy Options, ReadWriteWeb, June 29, 2009, available at http://www.readwriteweb.com/archives/a_closer_look_at_facebooks_new_privacy_options.php [last check, Jun.5, 2010]; Singel, R., (2007), *Private Facebook Pages are not so Private,* Wired magazine, available at http://www.wired.com/software/webservices/news/2007/06/facebookprivacysearch [last check, Jun.5, 2010]; Carole, M., (2006), *Privacy Fears Shock Facebook*, Wired magazine, available at http://www.wired.com/science/discoveries/news/2006/09/71739 [last check, Jun.5, 2010]; Bruce, C., (2007), *CIA gets in Your Face(book)*, Wired magazine, available at http://www.wired.com/techbiz/it/news/2007/01/72545 [last check, Jun.5, 2010]. See,

also, related video posted online and titled *The Truth about Facebook!*, September 6, 2007, available at http://www.youtube.com/watch?v=B37wW9CGWyY [last check, Jun.5, 2010]. See, also, sarcastic video on Facebook, titled *FaceBook in Reality—idiotsofants.com and BBC's The Wall*, April 28, 2008, available at http://www.youtube.com/watch?v=nrlSkU0TFLs&NR=1 [last check, Jun.5, 2010].

[145] Facebook Inc., plans to go for an I.P.O. See more, Vascellaro, J., (2010), *Investors Bet on Price of Facebook IPO*, Wall Street Journal, March 4, 2010, available at http://blogs.wsj.com/digits/2010/03/04/investors-bet-on-price-of-facebook-ipo [last check, Jun.5, 2010].

[146] RISEPTIS Report, (2009), ibid.

[147] ENISA Position Paper No.1, (2007), ibid.

[148] There is disagreement about it. There are those who support that rather than rushing to generate industry compliance with "soft law" which mandates software defaults, or even considering legislation of a more traditional variety, we should be doing nothing at all. See, for example, Edwards, L., and Brown, I., (2009), *Data Control and Social Networking: Irreconcilable Ideas?*, Harboring Data: Information Security, Law and the Corporation, A. Matwyshyn, ed., Stanford University Press, available through http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1148732 [last check, Jun.5, 2010].

[149] Vice-President of the European Commission and Commissioner Viviane Reding has already started negotiations between the E.U. and the U.S. aiming at reaching deal between the two parties regarding founding principles for privacy protection and data subjects' right. The European Commission adopted a mandate to negotiate a new personal data protection agreement with the U.S. It will be the first time that the E.U. and the U.S. negotiate together high data protection standards for their citizens whenever data is transferred and processed to fight crime and terrorism. See related video titled *Commissioner Reding presents plan for EU-US data protection deal,* May 26, 2010, available at http://ec.europa.eu/avservices/video/video_prod_en.cfm?type=details&prodid=14252 [last check, Jun.5, 2010]. The European Parliament, in a resolution on March 26, 2009, called for an E.U & U.S. agreement that ensures adequate protection of civil liberties and personal data protection. See Resolution 2010/C 117 E/32 of the European Parliament available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:117E:0198:0206:EN:PDF [last check, Jun.5, 2010]. In December 2009, the European Council invited the Commission to propose a Recommendation "*for the negotiation of a data protection and, where necessary, data sharing agreements for law enforcement purposes with the US."* See Council of the European Union, *17024/09, The Stockholm Programme—An open and secure Europe serving and protecting the citizens,* available at http://www.se2009.eu/polopoly_fs/1.26419!menu/standard/file/Klar_Stockholmsprogram.pdf [last check, Jun.5, 2010].

[150] European Commission, (2010), ibid., *COM(2010) 245*, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF [last check, Jun.5, 2010].