# Facebook as a Challenge to Privacy

by Fereniki Panagopoulou-Koutnatzi
LL.M. (Athens University), M.P.H. (Harvard University), Ph.D. (Humboldt University)
Email: ferenikipan@yahoo.gr

## I. Introduction

Facebook, a significant technological innovation introduced in February 2004, and the primary online social networking site today, offers a dynamic, new dimension to online services. However, it also poses a new challenge to individual privacy. Given that Facebook members are asked to provide a comprehensive personal profile to sign up for the site, including photographs and quite persona background information about themselves, Facebook has collected a vast database (a "psychogram") of its estimated 600 million active users. This information includes date of birth, political, religious and philosophical views, contact information, gender, sexual orientation, marital status, favorite books and movies, educational and professional backgrounds, and photographs of members and their friends (often "tagged" with friends' names). Privacy advocates and others raise concerns that this rich dataset is available to advertising companies (which can collect and send advertisements tailored to the idiosyncrasies of each user), government agencies, political parties, and scam artists and criminals looking to hoodwink people, rob them, and seduce young girls and boys, etc. Facebook executives' response to concerns about its collection of users' personal data is that this is posted willingly by its users (*data subjects*) and thus is an acknowledgement that this information is "public" or quasi public. The privacy issue is further complicated, however, since some personal data is distributed by Facebook, and its users not only in the Facebook community (its members), but also beyond the Facebook audience. This paper analyzes the impact of Facebook, a relatively new worldwide phenomenon, on the protection of privacy worldwide.

## II. Defining privacy

Presenting a simple, uniform definition of privacy is difficult because it encompasses two basic concepts — personal control and dignity (Whitman, 2004). American legal thought places great importance on privacy as the *control of personal information and personal autonomy*, while European legal thought places value on *dignity* and the *fundamental right* to privacy (Levin & Nicholson, 2005).

### 1. Privacy as control of personal information and autonomy

Concerns over the right to control our personal information is inextricably connected with the spread of information technology. As early as 1890 Louis Brandeis, a future U.S. Supreme Court Justice, and his law partner, Samuel Warren, defined privacy as the right "to be let alone" (Warren & Brandeis, 1890). This issue stemmed from the growing use of Kodak cameras at the time, and the invasion of privacy posed to individuals because newspapers had begun publishing photos, some of which compromised the reputations of noted individuals. The main purpose of the

right to privacy in the U.S. context is that the *individual alone* should hold the right to monitor, review and control his/her personal information (Levin & Sanchez, 2009). Legal scholars argue that the individuals' choice to keep certain information private and to disclose whatever they wish is crucial for safeguarding their independence, which in turn, allows them to freely select their own "projects" of life (Benn, 1971).

Another dimension of privacy is the right to control which areas of our lives, and/or which information should become visible to others, and if so, when and how we wish it to enter the public sphere (Parker, 1984). Privacy includes the individual's determination of when, how, by whom and to what extent information is communicated to others. What is crucial here is the right of individuals to control their personal information. Therefore, Facebook users who display very private photos of and information about themselves and without choosing (i.e., clicking on the user's option for) restrictive privacy settings on their Facebook pages can become victims of their own reckless behavior (Sanchez & Abril, 2009).

**2. Privacy as dignity**

According to this perspective, privacy is an expression of the universal right to human dignity. Therefore, the law must protect individuals' privacy according to the principle of non-invasion into the individual's personality (Warren & Brandeis, 1890). A further extension of this view asserts that privacy must serve a fundamental principle: respect for human dignity, integrity and independence (Bloustein, 1964). The violation of privacy exposes the individual to public view and public control, and violates human dignity (1964). Under this view, the violation of dignity encompasses the individual's development of personality and "inner world". In this sense, privacy includes the right of individuals to keep certain aspects of their lives confidential and thus hold present different personalities based on the circumstance. Protecting individuals' privacy is necessary because individuals may wear different masks (visors), each one appearing in different circumstances and contexts (Levin & Sanchez, 2009). Without safeguard for concealing our various masks, the individual can be negatively impacted.

**3. Risks of privacy in cyberspace**

The publication of personal data on the Internet poses particular risks to the individual. These risks are associated with the nature of the Internet as a universal medium that offers users access to unlimited information in millions of databases (government, commercial and private), media publications and personal web pages through the use of search engines such as Google. Given that Internet access is, in most of the cases, free, providers of various online content services sell advertising and other marketing strategies to cover their operating costs. Hence, most website-based organizations, advertisers and businesses want to assess and measure the effectiveness of their marketing and advertising tactics by monitoring Internet users' and their website visitors' online behavior. They use this data primarily for commercial purposes, and can gather such information via tracking software, of which users are generally not aware. Consequently, the "free of charge" sites that many users visit and use may in fact not be free, because unbeknownst to them, they are often "paying" by giving out personal data (name, email address, personal preferences) to secondary use sources such as marketing firms that collect and sell users' interests and buying habits (Rome Memorandum, 2008).

Also, various web servers store files regarding the data connection and number of visits users make to websites in order to measure the success of the website and tweak the site to increase user hits or visits. This clandestine tracking (spying, really) is not harmless. Such tracking services can assess which websites users visit and identify the users' IP address and gain further personal information (names, addresses, phone numbers) via IP providers, who often sell such information to marking firms. Each browser gives information about the user's country of origin and type of computer they use (brand, speed, memory, etc., which can be correlated to income levels and expertise). Therefore, a person who visits a webpage provides information to the owner of the visited site. Furthermore, through the search engines one can research and collect data about a person from different websites.

Another important point is that once information is published on the Internet, it can always be retrieved as it remains indefinitely in electronic storage caches. That is, once data is published, it may stay there forever, even when it has been deleted, because the original information remains archived on most search engines via the cache function, or by other data collection processes such as third-party copying (Rome Memorandum, 2008).

The Internet was developed in the 1980s to provide information and communication capabilities to anyone with Internet access. In the present phase though, the Internet is developing rapidly not only as a tool of communication (email, Facebook, the news media), but also for education, shopping, investing, gambling, dating, gaming, research, and banking to name a few. Internet access is both necessary and ubiquitous in all segments of modern life and is the leading information disseminator across all age groups, socioeconomic sectors and nations (though developed nations' use is far greater than that of developing nations). Businesses, governments and individuals collect and store personal information on the Internet by such as passport, social security, ID and tax numbers; dates of birth, fingerprints, credit card numbers and spending habits, credit scores, purchase histories, user Internet site preferences, newspaper articles (present and past), news media videos and photos, e-commerce and online auction data, social network and dating service profiles, personal blogs, research papers, and private photographs stored in individual's "private" file hosting websites. In Greece personal information on public sector of employees, such as job dismissals, salaries, work absences due to personal and business reasons, is collected and made available to the public online (Art. 2 of Greek Law 3861/2010 on public sector transparency mandates the publication on the Internet of a great number of public employees' administrative acts). The general public began using the Internet in the early 1990s but by the late 1990s, an intense debate had arisen regarding the free flow of personal information following misuses of private data and breaches of privacy committed by individuals, governments, corporations and nonprofit organizations.

## III. Privacy on Facebook

### 1. European Network and Information Security Agency (ENISA) Security Issues and Recommendations for Online Social Networks

This paper provides an overview of security issues in the social networking realm, highlights the major threats and recommends different types of action and best practices to reduce user security risks. It is addressed to corporate and political decision-makers as well as to social network application-providers such as Facebook and LinkedIn and Twitter. It also seeks to raise the awareness among political and

corporate decision-makers of the legal and social implications of the new social networking technologies. In particular, its findings have important implications for education and data protection policy. The examples used in this paper, although derived from specific social network sites (SNSs), primarily Facebook, are intended as examples only and are not aimed to single out a specific provider for criticism or praise. The paper concludes that SNSs have clear benefits to society, not only because they herald the end of passive media (a top-down approach where the general public *passively receives* news and information from the media corporations, but also because they democratise the media, and bring free, interactive user-generated content to anyone with an Internet connection.

Social networking is fundamentally an Identity Management system. If used for its intended purposes, it can enhance data privacy over and above more established mechanisms such as blogs. If not, however, it provides a dangerously powerful tool for spammers, unscrupulous marketers and others to take advantage, often criminal advantage, of users. New technologies such as online face-recognition tools, combined with the false sense of intimacy often created by SNSs, can lead to a serious erosion of personal and even physical privacy. Those who generate SNSs should pay attention to security and privacy laws in the development of code and data-handling policies. Most importantly, users should be educated in how to use social media safely via online awareness-raising training on the social networking sites themselves and in schools (elementary to university level) targeted at students, parents and teachers. This would also address the increasing danger of a 'digital divide' between those with the know-how to join in the 'social-software revolution' and those without. It requires a culture-shift in educators from the "beware of the dragons" scaremongering attitude behind efforts to ban SNS usage to a more realistic attitude of encouraging sensible, well-informed use. Finally, education is a matter for governments as well as internet service providers (ISPs) and end-users. Legislators and policymakers are currently not equipped with the information or technological savvy to address many of the challenges of social media. According to the recommendations of ENISA, Education policy should reflect the urgent need to educate both young and old users, students, teachers and parents on how to benefit from SNSs without suffering their downsides. Legislation should be reviewed and interpreted to fit the new paradigms with which we are faced.

## 2. Report and Guidance on Privacy in Social Network Services: The Rome Memorandum of 2008

The Rome Memorandum Working Group has made many recommendations to regulators, Internet content providers and social network services users. Its **recommendations to European Union regulators** include:

1) *Introduce the option of the SNS user's right to use a pseudonym* — to act in a social network service under a pseudonym — where not already part of the regulatory framework.
2) *Ensure that service providers are honest and clear* about what information is required for the basic service use so that users can make an informed choice of whether to sign up for and use services, and that users can refuse any secondary uses (through opt-out options), specifically by (targeted) marketers. Note that consent of minors in most countries is not valid and thus creates serious problems for children who use popular SNSs, their parents and the SNSs themselves.

3) *Provide an obligation to notify SNS users of data breaches.* To address the growing risks of identity theft, users must be notified of any data breaches. At the same time, such a measure would help regulators gain information on how well companies secure user data, and provide an incentive to further optimise their security measures.
4) *Rethink and accordingly amend the current regulatory framework* with respect to control of personal data (including third-party data) published SNS, with a view to placing more responsibility for personal data content on SNSs to the SNS providers.
5) *Improve integration of privacy issues into the educational system* because providing personal data online has become part of modern daily life especially for young people, thus privacy and tools for informational self-protection must become part of school curricula.

In 2008, the Rome Memorandum Working Group also recommended that **SNS providers** offer the following:

1) *Provide transparent and open information to users.* Even if this information is displayed when a user signs up for a service, and can be accessed and changed later if the user so wishes, the goal of informing users about the potential (negative) consequences of their actions while using such a service (e.g., when changing privacy settings for a collection of photos) may be better served by built-in, context-sensitive features that would deliver the appropriate information based on user actions. User information should specifically include information about (i) the jurisdiction under which the service provider operates, (ii) users' rights to access, correct and delete personal data, and (iii) the business model applied for financing the service.

   Also recommended: Information should be tailored to the specific needs of the targeted audience (especially for minors) to enable them to make well-informed decisions. Information provided in the user agreement should also refer to third party data: Providers of social network services should in addition to informing their users about how they use their personal data, also provide rules on how the users should handle third-party information contained in their profiles (e.g., how and when to obtain the data subjects' consent before publication, and the possible consequences of breaking the rules). In particular, the huge quantities of photos in user profiles that show other people (in many cases even tagged with friends' and colleagues' names and/or links to their profiles) add more layers of concern as current practices often do not comply with existing legal frameworks governing the right to control one's own image. SNSs are also encouraged to provide candid information about all information security risks, and possible consequences of publishing personal data in a profile, as well as about possible legal access by third parties (e.g., law enforcement, the courts).
2) *Introduce the creation and use of pseudonymous* profiles as an option, and encourage its use.
3) *Meet promises made to users:* A conditio sine qua non for fostering and maintaining user trust is to provide clear information about how their information may and will be used by the service provider, specifically regarding sharing personal data with third parties such as marketing companies.
4) *Use privacy-friendly default settings as a key means to protect user privacy:* In today's practice, only a minority of SNS users make changes to default settings including privacy settings. The challenge (and obligation) for service providers is to

design settings that offer a high degree of privacy *by default* without making the service unusable or frightening off users. At the same time, usability of setting features, along with explanations, is key to encouraging users to choose their settings.

*5) Improve user control over profile data.*

*6) Introduce appropriate complaint mechanisms* (e.g., to "freeze" contested information or pictures) where they do not already exist, for social network users, but also with respect to third-party personal data. Timely responses to user complains is important. Measures may also include a penalty mechanism for abusive behaviour with respect to the use of profile data and third-party personal data by users (including barring users from sites if they violate the rules).

7) *Improve and maintain information system security*. Use recognised best practices in planning, developing, and running SNS applications, including independent certification.

8) *Devise and/or further improve measures to prevent illegal activities, such as spamming and ID theft.*

9) *Offer encrypted connections for maintaining user profiles*, including secured log-in procedures.

10) *Respect the privacy standards of the countries where SNS operate.*

The Working Group's recommendations for **SNS users** include:

*1) Use caution* and think carefully before publishing personal data (specifically names, addresses, ages, and telephone numbers) in a social network profile.

2) *Think carefully about using one's real name in a profile.*

3) *Respect the privacy of others*. Be especially careful when publishing personal information about others (including pictures, particularly tagged photos), without first getting their consent.

4) *Be informed* about the SNS's operations, jurisdiction, regulatory framework for protecting privacy and whether it has allegations of abuse.

5) *Select high-level privacy settings*. Restrict availability of information as much as possible, especially with respect to indexing by search engines.

6) *Use different identification data* (e.g., login ID and passwords) than those used on other website user accounts (e.g. for e-mail or bank accounts).

7) *Use opportunities to control* how a service provider uses personal (profile and traffic) data. For example, always opt out of marketing options.

8). *Teachers and parents should pay attention to the activity of children on the Internet*, especially when using SNSs.

## 3. The Opinion 5/2009 of the Article 29 Working Party on the protection of individuals with regard to personal data

The Opinion of Working Party (established by Article 29 of Directive 95/46/EC as an independent EU Advisory Body on Data Protection and Privacy, whose tasks are outlined in Article 30 of Directive 95/46/EC and in Article 15 of Directive 2002/58/EC) focuses on how the operation of social networking sites (SNS) can meet the requirements of EU data protection legislation. The Opinion is principally intended to provide guidance to SNS providers on the measures that must be in place to ensure compliance with EU law. The Opinion notes that SNS providers and, in many cases, third-party application providers, are data controllers with corresponding responsibilities towards SNS users. The Opinion states that many users operate within a purely personal sphere, especially when contacting and

communicating with people while managing their personal, family or household affairs. In such cases of household affairs, the Opinion deems that the "household exemption" (of Art. 3 par. 2 of Directive 95/46/EC) applies and the regulations governing data controllers do not apply. The Opinion also specifies circumstances whereby the SNS user's activities are not covered by the household exemption. The dissemination and use of information available on SNSs for other secondary, unintended purposes is of key concern to the Article 29 Working Party. The opinion mentions cases in which activities of some SNS users may extend beyond a purely personal or household activity, for example, when the SNS is used as a collaboration platform for an association or a company (sec. 3.1.1). Furthermore when access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the SNSs or the data is indexable by search engines, access then extends beyond the personal or household sphere (sec. 3.1.2). The application of the household exemption is also constrained by the need to guarantee the rights of third parties, particularly with regard to sensitive data. In addition, it must be noted that even if the household exemption applies, a user might be liable based on the general provisions of national civil or criminal laws (e.g., defamation of character, liability in tort for violation of personality, penal liability) (sec. 3.1.3).

Robust security and privacy-friendly default settings are advocated throughout the Opinion as the ideal starting point for all SNS services. Controllers must take the appropriate technical and organisational measures, "both at the time of the design of the processing system and at the time of the processing itself" to maintain security and prevent unauthorised processing, taking into account the risks represented by the processing and the nature of the data (sec. 3.2). The Working Party recommends that SNSs provide adequate warnings to users about the privacy risks to themselves and to others when they upload information on the SNS; SNS users should also be reminded that uploading information about other individuals may impinge upon their privacy and data protection rights; SNS should also advise their users that if they wish to upload pictures or information about friends and associates or others, t the individual's consent is necessary (sec. 3.3). Access to profile information emerges as a key area of concern. When accessing personal data via a third party's Application Programming Interface (API) on behalf of a user, third party services should (i) process and store data no longer than necessary to perform a specific task and (ii) perform no operations on imported user contacts' data other than personal usage by the contributing user (sec. 3.6.2).

The Working Party also addressed topics such as the processing of sensitive data and images, advertising and direct marketing on SNS, and data retention issues. The Working Party Opinion also outlined recommendations on how SNSs should handle sensitive data, which includes racial/ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health, sex life or sexual orientation. Sensitive personal data may only be published on the Internet with the explicit consent from the data subject or if the data subject has made the data manifestly public him-/herself. In some EU Member States, images of data subjects are considered a special category of personal data since they may be used to reveal racial/ethnic origins or to deduce religious affiliations or health data. The Working Party in general does not consider images posted on the Internet to be sensitive data, unless the images are clearly used to reveal sensitive data about individuals. As data

controllers, the Working Party recommends that SNS should not share any sensitive data about SNS members or non-members without their explicit consent. If a SNS user profile query list asks any questions relating to sensitive personal data, the SNS must make it very clear that answering such questions is voluntary (sec. 3.4).

Key recommendations focus on the obligations of SNS providers to conform with the Data Protection Directive and to uphold and strengthen user rights. It is of paramount importance that SNS providers inform users of their identity from the outset and outline all the purposes for which they collect and process personal data. Particular care should be taken by SNS providers with regard to processing personal data of minors.

Data Protection Authorities worldwide have already begun some interesting initiatives that focus on awareness-raising regarding SNS and possible personal data sharing risks. The Working Party also encourages further research on how to address the difficulties surrounding age verification (particularly to prevent use by minors who are not of age to legally agree to consent) and proof of informed consent in order to better address these challenges. Based on the privacy considerations for minors, the Working Party recommends that a multi-pronged strategy should address the protection of children's data in the SNS context. Such a strategy might be based on SNS use and personal data awareness-raising initiatives (e.g., via schools, the inclusion of Data Protection-basics in educational curricula, the creation of ad-hoc educational groups to explore strategies and tools to educate children, the collaboration of national bodies to address these concerns), which are necessary to ensure the active, safe involvement of children (sec. 4). The Opinion recommends that users should upload pictures of information about other individuals, only with the individual's consent; it also recommends that SNS have the duty to inform users of the privacy rights of others.

## 4. Unique characteristics of privacy on Facebook

The definition of privacy in terms of Facebook is based on the degree of *privacy expectations* of the Facebook user. Personal profiles on Facebook vary and are based on what an individual chooses to present to the public or his/her Facebook "friends". Anonymous postings on Facebook through the use of pseudonyms is quite common and while it protects freedom of speech, anonymity makes it difficult to identify persons responsible for damaging or illegal postings, libel and other crimes. Although many users can protect their personal data by activating the privacy settings (e.g., by choosing an option to limit their information displayed to be viewed only by their Facebook "friends"), many are unable to monitor the information posted by others [by their Facebook "friends" about them, information their friends have gleaned from their "friends only" postings. Furthermore, the fact that Facebook allows users to decide for themselves regarding the degree of protection of their privacy leads to the risk that those who are more familiar with technology and the Internet will take effective protective measures, but that novices will not know how to do so; some might not even know what "privacy protection" means.

In this new digital age, Internet users should be aware that any online postings of personal information in private email and in public or semi-public sites like Facebook, may not be protected by privacy rights. The communication of "private" information to unwanted audiences is extremely likely, through direct or surreptitious

means. For this reason, the proposed privacy settings of social networks should be restricted for users (in dubio pro protectione) and if the user has chosen to make a Facebook page or blog or write an opinion piece and publish it in the newspaper or online, he/she should be construed as agreeing to make it public for everyone (e.g., if a writer or politician publishes photographs and text, he/she has thus chosen a wide audience and can not claim privacy protection); thus he should deactivate his/her SNS restrictive privacy settings. Requiring restrictive privacy settings by default should not be considered paternalistic treatment of users, as some have claimed. They are proposed given that many Facebook users sign up for the service without having the appropriate expertise to protect their personal data online and without reading the fine text often written in thick legalese in small print in long, online user agreements. This lack of knowledge or failure to carry out "due diligence" on the user's part can lead unsuspecting users to disclose data to a wide range of people without intending to. The principle of in dubio pro protectione does not apply, unfortunately to Facebook. On the contrary, the legal onus is on the users to restrict their Facebook and other online SNS privacy settings themselves, *even if they are not aware of them.* In this way Facebook establishes a presumption that the user *wishes to disseminate information* and does not *wish to protect* private information from others.

Along with the mandatory default of restrictive privacy settings to protect users' personal data it is also of crucial importance for Internet user groups and data protection authorities to raise the public's *online privacy awareness* and to educate it regarding on personal data protection strategies. Of great significance here are the information campaigns of the various data protection authorities. The campaigns should not, however, be the sole responsibility of those authorities. Schools should also play a very important role in educating students. Schools, from the primary grade level to universities, should not discourage students from participating in Facebook or other SNSs but rather educate students, teachers and parents on how to reap the benefits of Facebook and avoid any negative impacts.

Existing security risks of Internet services add to the risk of SNS use and further raise the level of risk, and could also develop "flavours" specific to social network services.

**5. Disclosure of personal data by the users**

Many service providers and SNSs promote their services as bringing innovative communication structures from the "real" world into cyberspace, making it easier for users to connect with new "friends" around the globe and around the block. Many Facebook users feel it is safe to publish personal data on Facebook, as this seems simply like sharing information with friends but in a new way. However, a closer look at some Facebook features reveals that this comparison has some weaknesses, including the notion of "friends", which in Facebook may substantially differ from the more traditional friendship, because cyber friends may never meet in person and get to know each other in real time. Thus, building trust is a more difficult process since interactions are all in cyberspace and not be "tested" necessarily in real time and space; also Facebook "friends" could be using aliases and "friends of friends" may not in actuality be friends (outside of cyberspace) because the Facebook community is vast and despite its name, friends are oftentimes faceless unknown entities. Thus, Facebook friends are not in fact similar to real-life friends that we meet at work, in school, in the sports arena and via actual friends. If Facebook administrators do not fully inform users about how their profile information is shared

and what users can do to control how it is shared, they may be lured into thoughtlessly sharing their personal data they would not otherwise share (Rome Memorandum, 2008).

The majority of Facebook users does not hesitate to post a wide range of personal information including their real names, their home towns, school or university from which they have graduated, their marital status, their interests, favorite music, films and books, their political views, and often photos of themselves. This is a self-exposure (Mitrou, 2009). Some users' reluctance to disclose personal data and especially their true names and photographs reflects the desire to network easily with other users. Through the Facebook application, a user can achieve a comprehensive outline of the data subject. A fully completed Facebook profile includes approximately 40 categories of information including name, date of birth, political and religious views, contact details, gender, sexual orientation, marital status, favorite books, favorite movies, educational level and institutions attended, and professional experience, giving other users a clear and rounded picture of the person. Also, Facebook offers its users several tools for finding potential friends and professional contacts (Cf. http://www.facebook.com/help.php?page=441 (propose contacts to the current contacts)**,** http://www.facebook.com/findfriends.php (contacts finding); Facebook Blog, http://blog.facebook.com/blog.php?post=15610312130 (Tips from Facebook), accessed 15.05.2011). Further Facebook applications offer a wide range of information about the user such Facebook "wall posts". Through a wall post users can get information on both the person who posted the information and the user (e.g., that a user is on holiday in an exotic island for two weeks). A tag in a photograph can reveal as much information about the person, his/her friends and the places that s/he has visited. Games on Facebook's Lexulous reveal the level of the user's vocabulary. The list of the pages and groups in which the user is registered indicate their preferences and views. Participation in Facebook quizzes reveals the user's level of knowledge, and views and preferences in politics, music, culture, to name a few. A user can participate in a quiz just for fun without realizing that the answers s/he gives in these quizzes reveal the user's likes and dislikes; the Facebook profile is essentially a psychogram of the user and provides rich information for those seeking data for marketing, political, fundraising and other purposes.

It is however remarkable that in many cases, Facebook users accept invitations of friendship from unknown users and as a result they share with unknown people their personal data, such as contact information and photos. In many cases, employers, before hiring an employee, evaluate the candidate via their social network pages and postings, along with doing a Google search of the individual. In this way they can evaluate the candidate as to whether his/her profile matches the firm's "corporate personality". According to CareerBuilder.com, 12% of the 1,150 hiring managers have admitted that they have surveyed the social network pages of candidate employees and 63% decided *not* to hire candidates based on findings from their social network pages. Also American Bar Association chapters report that lawyers check the SNS profiles of candidate jurors or witnesses in proceedings in criminal and civil matters such as divorces to see if they will have the attitude or hold the "correct" views for their purposes. Furthermore, banks check the SNS profile of candidates and employees to determine their reliability, personal activities, and preferences, and university admissions officers admit to checking the profiles of candidates for admission (Piskopani, 2009). Furthermore, employers report checking the Facebook pages of employees who have requested medical leaves to see if they are on a pleasure trip or indeed at home sick (of course, employees can post false information

to deceive their bosses as well); if discovered to be lying, the vacationing employee can be reprimanded for lying and for publishing private personal data with his own responsibility.

Many examples of unintended data disclosure occur on Facebook. A striking example is in the personal relationship realm: a husband may tell his wife that that he was at work when he was out late, but via posts on his Facebook pages, the wife may discover that he was partying late at a nightclub. Some may argue that the purpose of the right to privacy is not to protect delinquent behaviours. The purpose of privacy law is to protect the privacy of individuals because even if conduct is lawful, but something that the individual would like to keep hidden, they deserve protection, which stems from the right to protect the private sphere of a person. However, SNS users should realize that if they willingly reveal personal information, they cannot claim privacy of this information.

**6. Disclosure of personal data to a wider-than-intended audience**

What happens if Facebook users wish to disclose their personal information only to a specific, select circle of "friends", but Facebook makes available their private information (intentionally or unintentionally) without their knowledge to a wider group? According to the privacy policy of Facebook, it can reveal user information only to law enforcement officials with legitimate rights to it (e.g., via subpoena, warrants or court orders). Facebook can also communicate information to users when it is necessary to fulfil a legal obligation to protect users' interests or to prevent Internet crime, or to circumvent the possibility of physical violence to a Facebook member or non-member. Facebook must give notice to lawyers and law enforcement authorities before disclosing information.

What expectations of privacy do individuals have who display information on Facebook and make it accessible to a limited group of persons? Relevant here is U.S. case law on similar issues regarding disclosure of information to a wider circle than the targeted persons. According to the court's decision in *Sanders v. American Broadcasting Co* (978 P.2d 67, 72, Cal. 1999), the simple fact that a person has been seen with his consent by someone does not mean that he should be visible to everyone. Also relevant to this question is the *Multimedia WMAZ, Inc. v. Kubach (*443 S.E.2d 491, Ga. Ct. App. 1994). In this case the plaintiff appeared on a television program in which he had agreed to be interviewed about having AIDS. Prior to the program, the defendant agreed that the plaintiff's face would be disguised digitally to protect his identity on the air. Due to the negligence of the TV station's staff, the plaintiff was recognizable. The Court ruled in favour of the plaintiff.

It is clear what the American court's attitude would be in a case in which Facebook accidentally revealed private information. The fact that Facebook users make their profile available to hundreds and sometimes thousands of users would not override the plaintiff's reasonable expectation of privacy. Very few courts worldwide have rules that the claim of confidentiality is valid when one displays information in a publicly accessible medium like the Internet, without attempting to protect the information (United States v. Gines-Perez, 214 F. Supp. 2d 205, 224-26, D.P.R. 2002). The fact is that if users select restrictive privacy settings for their Facebook page, they should be entitled to greater privacy protection than users who do not activate restrictive privacy settings (Brandenburg, 2008).

While such cases are relatively clear-cut, what remains unclear is whether an effort to protect privacy through restrictive privacy settings on Facebook is sufficient to protect *the expectation of* privacy. It is very likely that if a user has made his/her profile accessible only to certain users but other users not entitled to access gain access, via authorised users (Facebook "friends' entitled to access) and in this way unauthorised users are able to join indirect access to the restricted page. For example, if an employer asks Employee B for access to his Facebook account in order to check the page of Employee A and thus gains "second party" access to private information of User A, and then fires Employee A based on facts gleaned from his/her Facebook page, does Employee A enjoy privacy protection, and is the employer or Facebook culpable for violating Employee A's privacy rights? The court could rule that due to Facebook's wide accessibility, it is extremely difficult for Facebook users to enjoy full privacy protection for their online postings and that the employer did not break privacy rules nor did Facebook by not stopping "second party" access (Cf. Reno v. ACLU, 521 U.S. 844, 1997).

**7. Photo tagging on Facebook**

In the digital era, it seems apparent that Internet users should bear the responsibility for the disclosure of personal data. But what about cases where the disclosure of personal data takes place without the knowledge or permission of the user? A good example here is the tagging (naming) of a person in a photograph without his/her knowledge, or desire or permission. In criminal proceedings in the state of Rhode Island, the prosecutor attempted to show, through photographs posted without the will of the defendant in a page of social network, that the behaviour of the defendant after an accident, which he had caused due to inebriation, did not demonstrate his repentance. Specifically, two weeks after the automobile accident the defendant displayed on his SNS page a photo of himself at a social gathering after the accident dressed as a prisoner wearing a shirt inscribed with "The bird of prison", thus making a joke about his possible imprisonment. The judge sentenced him to two years imprisonment stating that the photographs constituted evidence of the unrepentant behaviour of the accused shortly after the accident. In another case, a tag of a minor drinking alcohol in a Facebook picture led police to arrest this person for alcohol consumption (http://freedom-school.com/reading-room/unrepentant-on-facebook-expect-jail-time.pdf, accessed 15.05.2011).

The photo tags on Facebook and other social network pages raise serious concerns regarding the protection of privacy. Facebook has four levels of privacy protection regarding photos:(a) all "friends" (people who the user agrees to network with online), (b) "friends of friends", (c) friends, friends of friends and networks of the user and (d) all users. These options seek to prevent the invasion of the user's private sphere. The process of tagging (placing a name — first name or both first and family name) includes the automatic notification of the depicted person. When a Facebook user is tagged in a picture s/he is alerted automatically by an email from Facebook and s/he can ask to remove the tag (name) from the picture. It should be noted, however, that the depicted person has no room for reflection from the time of the tagging until the decision to keep or remove the tag of the photo. It is therefore very likely that until the depicted (tagged) person has read the e-mail, some other Facebook users will have seen the tagged photo and could have copied and saved the picture in their own personal file. The process of tag removal makes it much more difficult for users to discover the photo because, his/her face is still visible to other users who have access to pictures. Furthermore if other people tagged in a picture have not

chosen to remove the tag, the depicted person who is not tagged can be exposed to unwanted publicity. Therefore, the privacy protection via the tag removal mechanism is inadequate. Facebook receives numerous complaints daily about inadequate protection of privacy because it only allows the removal of a photo if a picture is offensive. A proposed solution to the affected user is to communicate with the "friend" who posted the offending photo and request its removal from the web site. Therefore, protecting the privacy of affected users is at the discretion of the user who posts pictures. However, because the user who posted the picture can refuse to remove the photo, there is a great gap in the protection of privacy. The question is, can the affected party enjoy some other form of protection of private life, other than suing him. Can the privacy law protect Internet users in a preventive way? Are there protection mechanisms that do not negate the positive attributes of Internet-based social networks? The fact is that even if Facebook is subject solely to internal controls, then the control options would be restrictive and focused primarily on removing offensive photos. One solution is for Facebook to be required by law to remove an offending photos if Facebook receives a complaint from a user or nonuser depicted in a photograph (details of valid complains would have to be worked out in detail). In this way the protection of the affected person would be more efficient than for the user to resort to suing the user who posted the offending picture. This would clearly place a great burden on Facebook as it would be required to remove offending pictures. Nonetheless, I propose this option as a necessary and appropriate measure to protect individuals who may be harmed by the content and photos placed on Facebook pages.

## 8. The consent of Facebook users — privacy protection

Facebook has argued that the user agrees to the terms of use before joining the social network site. Questions arise, however, as to whether users' consent is specifically expressed and informed. Consent is not an option for negotiating the transaction and user terms. It is a formality, a simple "click" in a box placed under a page of indecipherable legal language and fine print difficult for non-legal experts to understand. The fact is that most users do not read the terms of the privacy policy of most online user agreements of sites because they are complicated and incomprehensible and they are in a hurry to move on. The average Facebook user, for example, is unable to understand the terms and conditions of privacy and therefore does not understand what s/he consents to (Hashemi, 2009, p.153-4). Most people also do not understand the extent of data collected and recorded on Internet sites and SNSs. We should also not overlook the fact that most users are not aware of the possible uses (present and future) of the content and photos they post online and the potential economic value that others can glean from the acquisition and/or use of this information. According to Facebook, less than 25% of users modify the default privacy settings on Facebook (http://www.dallasnews.com/sharedcontent/dws/bus/stories/120907dnbusprivacy.1c47951.html, accessed 15.05.2011). This is not because users do not care about privacy, but because 25% are not aware of the privacy settings (Haynes, 2007), nor the terms of privacy they enjoy or could enjoy. It is also worth noting that Facebook administrators are constantly modifying protection of privacy terms without properly informing users and/or requiring users to renew the agreement. Information concerning the modification of Facebook's privacy policy can be found on specific information pages and alert and informed users must look for it. In other words, Facebook puts the onus on users to constantly check for changes in the agreement. It

seems that only the agreement that users sign is valid, not the updated ones that Facebook makes and does not send out to users to re-sign or approve.

## IV. Conclusion

Clearly Facebook provides very important social networking services that have impacted how society, particularly the 12 to 35 year-old age bracket, communicates and "connects". However, we should not ignore the privacy risks posed by Facebook. It should be the role of the law to meet this challenge and to transform the dangers of Internet technology from a privacy threat to a rational jeopardy (Alivisatos, 2004). The law must not only be shaped by technology, but it must also shape it. Furthermore, the courts must direct, control and limit emergency response technology and adapt to the current level of science and technology (Donos, 2004). However, the law came second in this story. First, those impacted by the risks of these new technologies brought suit against the "offenders" and then the law had to deal with the problems and respond to individual needs. This is logical, because the law does not have clairvoyance or predictive abilities. The fact is, however, that today's privacy laws are insufficient to protect privacy of Facebook users and those who are affected by that actions that threaten individual privacy. It is imperative that we redefine the concept of privacy for the Internet and that we reconceptualise social networks worldwide, given the globalization and power of the Internet.

# V. References

Alivisatos, N. K. (2004), Introduction in: "New technologies and constitutional rights", Athens-Thessaloniki, p. 7 ff.

Article 29 Data Protection Working Party (2009), Opinion 5/2009 on online social networking, online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf, accessed 15.05.2011.

Benn, S. I. (1971), Freedom, and Respect for Persons, in: J. Roland Pennock & John W. Chapman (eds.), Nomos XII, Privacy p. 1 ff.

Bloustein, E. (1964), Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 N.Y.U. L. Rev, p. 962 ff.

Brandenburg C. (2008), The Newest Way to Screen Job Applicants: A Social Networker's Nightmare, 60 Fed. Comm. L.J., p. 597 ff.

Donos, P. (2004), Technological jeopardy and protection of personal data, in: "New Technologies and constitutional rights", Athens-Thessaloniki, p. 23 ff.

ENISA Report, Security Issues and Recommendations for Online Social Networks, October 2007, online at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf, accessed 15.05.2011.

Haynes, A. W. (2007), Online Privacy Policies: Contracting Away Control Over Personal Information?, 111 Penn St. L. Rev., p. 587 ff.

Hashemi, Y. (2009), Note: Facebook's privacy policy and its third-party partnerships, 15 B.U. J. SCI. & TECH. L., p. 140 ff.

Levin A. / Nicholson M. J. (2005), Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground, 2 Ottawa L. & Tech. J., p. 357 ff.

Levin A./Sanchez Abril P. (2009), Two Notions of Privacy Online, 11 Vand. J. Ent. & Tech. L., p. 1001 ff.

Mitrou, L. (2009), Note on Case of the Court of 1st Instance in Thessaloniki, 16790/2009, DiMEE 2009, p. 400 ff.

Parker, R. (1984), A Definition of Privacy, 27 Rutgers L. Rev., p. 275 ff. (281).

Piskopani, A-M (2009), The protection of privacy of Facebook users, DiMME 2009, p. 228 ff.

Rome Memorandum (2008), Report and Guidance on Privacy in Social Network Services 43rd meeting, 3-4 March 2008, Rome (Italy) International Working Group on Data Protection in Telecommunications.

Warren S. /Brandeis L. (1890), The Right to Privacy, 4 Harv. L. Rev. (1890), p. 205 ff.

Whitman, J. Q. (2004), The Two Western Cultures of Privacy: Dignity versus Liberty, 113 Yale L.J., 2004, p. 1151 ff.