UNIVERSITY OF PIRAEUS
DEPARTMENT OF DIGITAL SYSTEMS
POSTGRADUATE PROGRAM: DIGITAL SYSTEMS SECURITY

Privacy in Social networks

Giannis Gkountelas
4/11/2013

Abstract - The protection of users' privacy in all aspects of technology is crucial. Social networks pose the most complicated and yet interesting case to study from a privacy perspective because users waver between their need to disclose as much information as possible and their desire for data security and privacy. These settings are most of the times vague and hard to understand for those unfamiliar with technology and for this reason many aspects of security and privacy can be jeopardized. For the needs of this study, the leading social network is examined. The paper is organized as follows: firstly the reader is introduced to the scientific area of social networks. Then privacy issues and implications that have risen over the years are presented with the examination of Facebook's privacy issues and practices following. Lastly after reviewing proposed countermeasures, ways of protecting data based on the prevailing settings and policies are offered and conclusions are made.

Keywords: Facebook, social networking site, privacy, personal information, data protection

Table of contents

Table of contents 3

Acknowledgements 6

1 Introduction 7

2 Social networks 9

2.1 Definition of social networks 9

2.2 Social networks services 9

2.3 Classification of SNS 12

2.4 Characteristics of SNS 14

3 Privacy issues on SNS 16

3.1 Information stored 16

3.2 Access to user's personal information 16

3.3 Threats 17

3.3.1 Privacy related threats 18

3.3.2 Information security threats 19

3.3.3 Identity related threats 20

3.3.4 Social threats 20

4 Facebook - the leader of SNS 22

4.1 Facebook – The web 2.0 phenomenon 24

4.2 Facebook services 25

4.2.1 Facebook 1.0.1 – creating a profile 25

4.2.2 Editing a profile 26

4.3 The evolution of Facebook's privacy policy 30

4.4 Users attitude towards privacy policies 35
4.5 Facebook privacy policy – an overview 36
4.6 Default privacy settings 38
4.6.1 Privacy by default 39
4.6.2 Users' approach towards privacy 40
4.6.3 User information 41
4.6.4 Apps and ads 42
4.6.5 Application of the Data Protection Directive to SNS and search engines 43
4.7 Major Facebook privacy concerns 45
4.7.1 User related privacy concerns 45
4.7.2 Facebook related privacy concerns 47
5 Countermeasures 53
5.1 Privacy Enhancing Technologies 53
5.2 Privacy by design – Privacy by default 54
5.3 Oppositions and conflicting interests 55
6 Raising users awareness 57
6.1 Reading a privacy policy 57
6.2 Recommended privacy settings for Facebook 59
6.3 General rules for social networking 61
7 Last thoughts and discussion 64
8 Conclusion 66
9 References 68

Acknowledgements

Sincere thanks are due to all the respected Professors of the University of Piraeus of the post-graduate program of Digital Systems Security and in particular to Ass. Professor E. Mitrou for her general supervision, constructive critique and guidance during the planning and development of this study.

1 Introduction

Social networks have grown larger over the last decades and are considered to be the landmark of the web 2.0 era. Nearly half of the users who have access to the Internet are members of at least one online social network. Sites like Facebook, MySpace, twitter, Google+, LinkedIn and many more have attracted users of all ages and backgrounds. Many users have integrated Social Network Sites (hereafter SNS) into their daily routing and practices as modern social networks offer various possibilities. Apart from the obvious social aspect they cover, which is to help people get in touch with others and socialize, they are used for news & entertainment, self-advertising and search for career opportunities.

Despite their popularity and mass usage SNS are related to many risks concerning both their users' privacy and data security. Data from different locations and sources are collected and aggregated by search engines, social networks aggregators (Spokeo, Pipl) and mass-ups (Poplfly) in applications that combine different types of information such as location data, photos, audio and other information that are available in a single view. Unauthorized access to this data can be identified as the major risk for users on SNS and derives, on one hand, from users' tendency to disclose great amounts of sensitive and private information on the SNS and on the other from the unfamiliarity with privacy settings which contain loopholes and fail to ensure privacy by granting access to third parties. Users on their vast majority tend to neglect or overlook these settings and over-share data that can be easily either stolen or used in many ways against them as there are other parties who would use these data in their favor. Thereby, users become potential victims of actions that can harm them not only in their digital/online presence but also in the real life.

Disclosure of great amounts of personal information followed by concerns about privacy has drawn attention onto social networking sites both from the research community and from the media. Due to the fact that information, that would be otherwise forgotten, can be stored for an indefinite period ENISA has stated that the Web 2.0 period has the "Hotel California impact" on users *"they can check out any time they like but they can never*

leave" (ENISA, 2007). The popularity and leading role of Facebook makes it an excellent candidate for studying what privacy can and should mean in the web 2.0 world.

This study aims to contribute to the privacy literature related to the field of social networks. For doing so, first an introduction is given to the scientific field of social networks and privacy issues are discussed. Then, Facebook's features are presented including a detailed analysis of privacy settings offered and threats that compromise privacy and have raised concerns are addressed. Finally, solutions for securing user's privacy and protecting data shared are proposed and conclusions are made.

2 Social networks

2.1 Definition of social networks

Social network is a term that comes from the scientific area of sociology and anthropology and its theoretical concept was first used in the social and behavioral sciences. Inventor of the term and first to define it was John A. Barnes back in 1954 by saying that social network is a social structure, which includes individuals or groups tied with the same type of activity, common interests, friendship or relationships (Barnes, 1954). Since then, it progressed and gained a lot of popularity as a concept eventually leading to be employed in other sciences as well, like network or economic sciences.

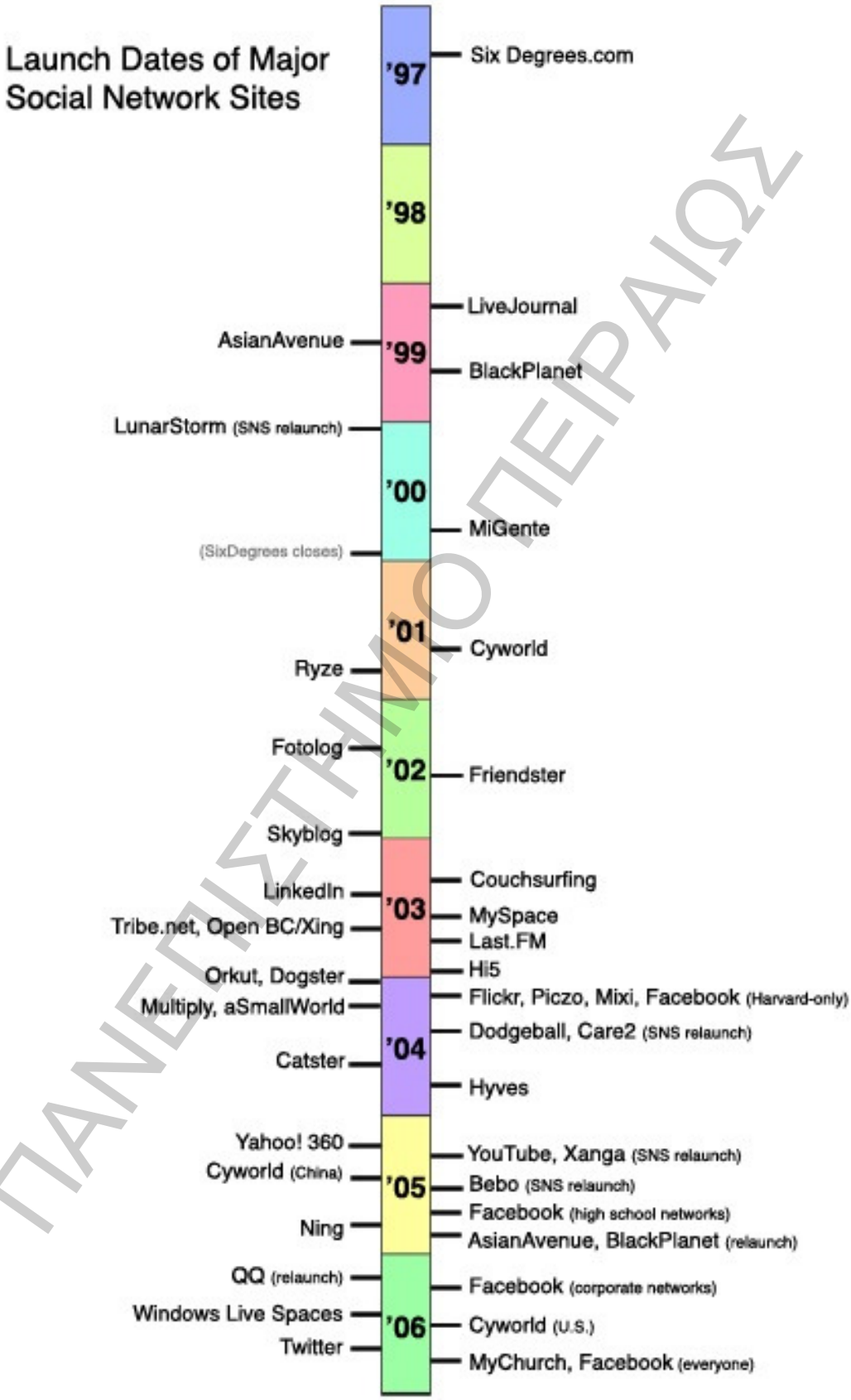
2.2 Social networks services

Social network sites are considered to be the most remarkable feature that has increased exponentially, not only in numbers but also in popularity, during the Web 2.0 era. Social networking sites (also described as "online social networks" or "social networking services"), as defined by Boyd and Ellison, are web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection and view and traverse their list of connections and those made by others within the system. When examined in the context of computer based communities, SNSs can be described as internet communities where individuals interact with others through profiles that represent their selves (Acquisti and Gross, 2006) while Wellman, on the other hand, characterizes SNSs as a set of social entities or people connected by a set of socially meaningful relationships (Wellman, 1997). The existence of various definitions suggests that there is no just one definition applicable to the term "social network" and it's up to the researcher to give his own interpretation depending on which scope he examines the matter.

In simple terms, they are online communities that allow people, through a built-up page, to create self-descriptive profiles and interact with other community members by creating a network of personal connections. For better understanding of the SNS's structure, imagine a network and think of the users as nodes and their connections as links. Through SNSs communication becomes easier and faster by bringing together digital communication

and real time publishing. In addition, SNSs support the construction of digital identities and help people promote themselves and interact with others.

The main motivation for users to join SNSs is communication and interaction with others. Researchers have shown that users primarily want to maintain relationships and interact with people who are already part of their extended social network rather than solely make new acquaintances (Boyd & Ellison, 2007) while according to Grimmelmann (Grimmelmann, 2008) people also join SNS in order to convince others to accept claims about their identity and to satisfy the need to belong to a community. Other popular activities include finding jobs, dates, sharing information and media (photos/videos/music), participating in events and group chats (Boyd and Ellison 2007, Dwyer et al., 2007). The first web based service that came closer to what Boyd and Ellison suggested was SixDegrees.com created in the late 90's marking the era of SNS. In the graph that follows, with some of the most notable SNS and their launch dates, it is pretty clear that the outbreak of SNS in the 00's didn't go unnoticed and received much attention and eventually SNS became part of the internet mainstream and leading force. (boyd and Ellison's timeline of major social network launch dates *Journal of Computer-Mediated Communication 13 (2008) 210–230 2008 International Communication Association*)



2.3 Classification of SNS

In scientific literature there are hardly any classifications for SNS which is strange due to the publicity and the studying they have received. Some technology based blogs offer relevant thoughts on the matter but in general it can be pointed out that the main criteria resolve around topic focus, services provided and purpose for which users decide to visit the SNS. A summarized categorization based on a certain study is presented below (Beye, Michael, et al. 2010)

SNS can be divided in two main categories:

- ***Broad-range or general purpose*** social network sites where all users are welcomed to participate regardless their interests and background as the main purpose of these SNS is to find old friends or make new ones and keep in touch with them. People commonly present their real-world identity in such sites. Sites whose primary purpose is sharing content (e.g. YouTube), invitation-only networks or sites where few reveal their true identity and real information about themselves (online gaming sites) don't fall into this category even if, some of these services contain features of general purpose SNS. Facebook, Google+, MySpace are some of the most notable SNS to belong in this category.
- ***Niche*** where users join to perform a specific activity that varies from job seeking opportunities and search for professional contacts to reuniting with old friends. Niche SNS can resolve around movies, sports, dating, entrepreneurship as follows

    1. **Business networking sites** specialize in maintaining professional contacts and searching for new jobs. Users share more professional information in these sites than personal information in order to find jobs and manage business relationships. LinkedIn, is the most popular business oriented network site.
    2. **Media recommendation sites** where users recommend/share films and music. Users interact with others based on similar interests and

tastes regarding movies, TV-series, music and books. Flickster is one of the most known media recommendation site.

3. **Private communication/Dating/Reunion sites** where people search for old friends from school, university. Such sites often require contact information only in order to endorse off line interaction instead of an online one. Classmates.com represents this genre.
4. **Informational/Educational/Academic sites** where people seek answers either to everyday problems or collaboration with others on academic stuff.
5. **Hobby or other activity focused sites.** Gaming focused social networks like Habbo and Gaia online allow their users to interact based on their favorite games, reading reviews/previews. Finally, CouchSurfing is designed to help students travelling abroad find accommodation.

Apart from these categorizations there are also others based on trust. This distinction contains two categories namely "Open networks" and "Gated Communities". In fact "Gated Communities" are more privacy oriented**.** This category consists of networks which are designed to be pseudonymous or implement strong parental control for safer children-browsing. In addition there are sites that are community-owned, suitable for those uncomfortable with the idea that their personal information is being gathered by a private company. Sites that can be classified into this category are Experience project, Imbee and Kaioo but they don't have a significant fan/user base yet. Other ways to distinguish between SNS are:

- **Source of revenue** where the SNS provider can earn revenue through subscriptions or data sales and advertisements.
- **Membership type** where subscriptions are open or by invitation only.
- **Wideness of user base** where the audience of a SNS is worldwide, national or regional or it attracts specific demographic or subculture.

2.4 Characteristics of SNS

Although SNSs may seem to differ regarding their intended use, their common characteristic consists of visible profiles that display detailed personal information along with many other common features (boyd and Ellison, 2007).

To begin with, after joining an SNS, the new user needs to create a profile to introduce himself/herself to other users in the network. The user is asked to fill out forms with identifying information such as name, gender, birthday, contact information (address/phone numbers), location information along with details about interests and educational and work background. Profile pages in SNS play the role of an identification card in real life and so a valid ID should have a picture of the holder. Likewise, nearly in every SNS users are encouraged to upload a photo.

Another common feature and crucial component of SNSs, is the connection of users with others they already know in real life or with people they meet in SNS for the first time. Friends/contacts/fans/followers all are terms used to describe these connections that can go one way or both ways. On one way connections no confirmation is needed and in most SNSs these ties are called fans or followers while on the other hand, confirmation is required from both parties. Keep in mind that the term “friends” doesn’t necessarily mean friendship in digital life as people connect with others for many reasons (work “friends”) (boyd, 2004).

Furthermore, SNSs offer ways to their users to communicate with each other and at least one of the following three is provided by any SNS: public, private and instant messaging. Public messaging involves posts to user’s profile or comments on photos and other activities and these posts are visible to everyone who has access to this particular profile. Private messages, on the contrary, are what their name suggests and are only visible to the recipient. Private messages are usually organized like emails are in an email account. Lastly, instant messaging is a feature where real time conversation is offered when users let others know they are online and available to chat.

Last but not least, the last common characteristic of all SNSs is that although their privacy features may have different approaches generally they abide to the rule “default all” meaning that profiles and information included are visible to anyone. Privacy doesn’t seem to be first priority in the development of SNSs and as will be seen below, these common features that enhance social networking can cause concern when we look at user privacy.

3 Privacy issues on SNS

Users need to reveal information in order to make use of the services provided by a SNS therefore there is a trade-off between services offered and privacy. Utilizing all features offered by a SNS is one thing but users should also keep in mind the risks that lurk while sacrificing privacy at the expense of more services and better online activity. There are examples where data is sensitive (medical, sexual orientation data) and the open nature of the SNS certainly doesn't favor privacy. How information is stored, along with who can access these data and the potential threats to users' privacy are being presented in this section.

3.1 Information stored

Information gathered can be either information shared or given by the user or information collected through online tracking (Davis Tremaine, Bloomberg, 2010). Information shared may include all kinds of information mentioned in the previous section (education/employment history, location info, personal info, photos, interests, connections) and generally has to do with the data users decide to provide willingly to the SNS in order to utilize some or all of its features. Information given has to do with the information generated through the interaction with the SNS and can be either knowingly or unknowingly revealed by the user (Gross & Acquisti, 2005). Information knowingly given includes data that derive from "liking" and posting stuff while unknowingly involves cookie information (text stored on a user's computer or mobile device containing information about credentials), the type of device and even what browser used to access the site along with the user location. Information may also be gathered from the actions of the user outside the boundaries of the SNS and includes tracking of which websites a user has visited along with actions he performed on these sites.

3.2 Access to user's personal information

At the same time, considering who has access to users' information is of equal importance. According to studies (Gross and Acquisti, 2005) there are three groups of people that have access to users' data in a SNS: the SNS itself, the users of the extended network and third parties.

The platform provider obviously has access to users' information. Even though the user can choose who can access the information shared, in some cases, the SNS has full access to user data, collecting for example the user's IP address and browser type and the information provided such as name and photograph is available not only in search results inside the SNS but also across the search engines (Google, Yahoo, Bing) (Ha, Techcrunch, 2013) (Webster, eHowTech).

Other users of the SNS also have the potential to cause privacy issues. It is possible that other SNS members leave an awkward comment on the user's profile or tag a picture portraying the user without his consent in an embarrassing situation. Privacy settings don't cover this aspect entirely so the best thing would be to know with whom information is shared and privacy terms between both parties agreed in order to avoid problems mentioned.

When talking about third parties we refer to entities that collect information either legally or illegally. Advertisers, under the prism of legality, gather personal information so they can better target their advertisements to those most likely to be interested in the product. Additionally, third party application developers who use personal information to personalize applications such as games, calendars may gain access to personal data published on profile in a more indirect way as they require confirmation by the user. On the other hand, there are always malevolent users lurking in the shadows in order to obtain personal information for identity theft purposes and harassment (Gross & Acquisti, 2005).

3.3 Threats

Another significant factor to be highlighted is the dangers that come along with the use of SNSs. Access to personal information by others can result in a wide variety of risks and threats associated with privacy and security. Every SNS user should be aware of the risks and threats related to the use of social networks. Apart from the classic threats which are common to all web applications such as identity theft and profiling there are others more specific to SNSs. The European Network and Information Security Agency (Enisa, 2007) has divided the threats concerning SNS into 4 major categories.

3.3.1 Privacy related threats

In this category there are threats that compromise data privacy and security and concern all the data and metadata that a user's online presence produces.

First threat to consider is the digital dossier aggregation. Information shared on profiles on SNSs can be downloaded and stored by commercial data brokers creating digital dossiers with tons of personal data. In addition, aggregated information is being sold to data-mining companies, marketing firms and credit reporting agencies for profit and advertising purposes. As a result, data provided on SNSs ends up to be used in a completely different way than the user initially had in mind. There are numerous reports where data available on SNSs backfired and resulted in missing employment opportunities, blackmailing and embarrassing the owner.

Then, there is the secondary data collection risk. Apart from all the information that can be gathered from a profile on a SNS, the usage of the network itself discloses certain information to the operator. Data like time and length of connections, IP address, number of times each profile was visited and by whom, messages sent and received and generally all activity done when joining a SNS. Additionally, that kind of information isn't only used by the operator to personalize the networks services but it can also be sold to third parties as mentioned before.

Another major threat is the facial recognition on SNS. One of the most popular activities on SNSs is photograph sharing. Vast majority of the users of SNSs have at least one photograph on their profile depicting them. Face recognition algorithms used in SNSs help others identify the profile owner either explicitly through labeled boxes with the name of the owner on images or implicitly through correlating two or more photos. This means that anyone who would have access to such tool could identify a specific person through different SNSs.

More to that, there is the Content-based Image Retrieval tool (CBIR). While face recognition helps detect the person who owns the data, CBIR helps detect the location photo was taken through the recognition of common objects in the photo even if the photo is edited (cropped, resized, rotated). It is easily understood that when location is compromised problems such as stalking, blackmail and unwanted marketing can arise.

Another important thing to consider is that when a user uploads a photo he is usually prompted to provide additional data concerning the place, the time and the people he was with. Even if the user is privacy-oriented himself and hasn't provided that information he could be in danger from other users who would be encouraged to tag him in the photo disclosing his personal data (name/email) and a link to his profile page. Furthermore there are cameras that not only leak the exact time and date photos were taken but also their serial number that could be used easily to identify the camera owner.

Lastly, one of most common misconceptions is that "deactivate account" actually means the complete deletion of the data available. Unless the user manually removes all comments, posts, photos posted both on his profile and his contacts' profiles, complete removal of data is unfeasible. Moreover, it is implied that all data is stored somewhere as when someone tries to deactivate his account he is reassured that if was to change his mind he could reactivate his account. This results in loss of control over personal data that can be damaging for user's reputation as embarrassing or incriminating posts can't be deleted.

3.3.2 Information security threats

This category includes variants of threats that are traditional and are usually encountered in network and information security.

One of the easiest and most common attacks to perform is spam. SNSs have grown popular not only for people who want to communicate with others but also for spammers who want to take advantage of such enormous user-base. Motif and techniques used (embedded links, mass friend requests/messages) remain the same and so do the problems caused (traffic overload, phishing, loss of trust inside the network).

SNSs are also reportedly vulnerable to XSS (cross site scripting) worms and viruses even though XSS, as an attack method, is considered to be of moderate severity. A XSS attack allows the attacker to do anything the victim will do on behalf of the victim such as reading his messages, viewing his private pictures, stealing account information and so on. The most notable XSS worm, SAMY was a major blow to MySpace's reputation as apart from the above caused a massive DOS to the site.

Additionally, as people use more than one SNS on daily basis the problem of keep up with the updates in each SNS occurs. SNS aggregators gather all data from all SNSs used into a single platform. No need to say that in this case privacy is diminished as an attacker can look into a broader base of data.

3.3.3 Identity related threats

This category includes techniques that are used to gain access to someone's private information in order to use them for illicit purposes.

First technique that is being acknowledged is spear phishing. SNSs make it relatively easy for anyone who wants to harvest information about a specific person due to the amount of personal data provided along with the person's contacts, habits and interests. Carefully crafted spear phishing attacks via SNS can result from compromised accounts to identity theft followed by reputation or even financial damage.

As mentioned before, an attacker could gather information regarding another user not only by using illicit means to gain unauthorized access but also in a legitimate way using SNSs features like friends. For the sake of popularity users often add/accept contacts without checking their authenticity. As a result the user ends up sharing information with people that can use it for their benefit.

Fake profiles are maybe the most common way to damage one's reputation. SNSs facilitate the use of fake profiles as in most cases all that is needed to create a profile is an email. Then, certain activities through this profile visible to a specific audience are all the attacker needs to humiliate and embarrass the victim. Fake profiles are also used for phishing (gain information about the person through his contacts) or marketing purposes.

3.3.4 Social threats

Social threats have to do with risks and dangers that can harm the victim mostly in his real life taking advantage of his online presence.

Up until the rise of SNSs a stalker would follow his victim or monitor his phone. Now with the use of SNSs stalker's job becomes easier as contact and location information are some mouse clicks away. With users revealing addresses, phone numbers, daily

schedules and informing their contacts e.g. that they are going at the movies, the loss of privacy is enormous.

Secondly, SNSs act as platforms where bullies can say things they might not usually say to someone in person as anonymity and less physical proximity act as a wall between the bully and the victim. None the less, the words and rumors that are shared are still just as hurtful. Bullies often feel more confident online and they can contact their victims any time, any place, day and night, not just in schoolyard. Cyber-bullying is a serious problem than needs serious observation as there have been documented incidents where victims resort to suicide. For example in 2009 a 14 year old girl committed suicide as a direct result of cyber-bullying (Dikeos, 2009). Another well know case was the case of Megan Meier (Megan Meier, Times Topics, 2011) where someone created a fake account and constantly teased Megan until she committed suicide.

Last but not least, as many users visit SNSs from their workplace attackers target employees who use them to gain access to sensitive data and bypass security mechanisms. Therefore, SNSs become tools in the arsenal of the attacker in order to craft social engineering attacks on employees who neglect privacy settings. Just by looking at the victim's contacts it's possible to find other employees or by searching the work history one could spot current or former employees which could be useful for social engineering against the corporation.

All things considered, unauthorized or unwanted access can have devastating effects in all aspects of the users' life sometimes resulting in irreparable situations both in real and in digital life. It is easily understood that anyone who willingly joins any SNS, in a way, compromises his own privacy regardless if he chooses to use any of the privacy settings provided. Threats are many and will always be there deriving from the unawareness of the users followed by privacy violators who will try to gain advantage from users' personal information. Privacy should be highly regarded and all these factors should be reviewed, for the users' benefit, prior to joining a SNS and the digital world.

4 Facebook - the leader of SNS

SNSs existed for at least 10 years and it was the success of Facebook that drew much attention and made SNSs global trends. Facebook is a social networking site that was founded in the USA in 2004, by a Harvard University student, Mark Zuckerberg. The site initially targeted fellow students at Harvard but later expanded to include other universities, colleges and high schools before letting anyone with an email address who is willing to claim to be 13 or older join (Tuunainen et al, 2009).

Facebook is the largest and fastest growing SNS which counts over 1.1 billion users in total and boasts approximately 665 million visitors every day. These users have uploaded so far 240 billion photographs and have created, more or less, 1 trillion connections. Furthermore, it is among the two most visited sites in the world constantly trading places with Google. It is also considered to be the 3rd most populous county in the world and it is expected that by 2016 it will have overtaken India and China due to its mind blowing growth rate of 77% annually ("Facebook may be the largest "country" on earth by 2016", 2013). Moreover, only 9 years after launching and less than a year after going public, Facebook made it to the Fortune's lists with the companies with the biggest revenue (Business Insider, 2013). These are only some of the statistics that show what significant and special role Facebook plays in the web market share and in the world in general.

Facebook's purpose (at least at first glance) is to help people constantly communicate with friends, coworkers, family members despite the distance between them. There lies the key difference that makes Facebook stand out of the other SNS. Facebook provides many more possibilities to make social networking a unique experience. It provides access to applications that enhance social networking and features like "Places" which help users find nearby friends based on location. Facebook isn't just another SNS platform where people solely meet old friends, socialize and make new acquaintances but it's the bridge between real and digital life. Moreover, with its many services, actions in real life that would otherwise stay there are transferred in the digital world with many consequences following them.

The following picture was published in Business Insider in 2012 (The 15 maps that explain the entire world, www.businessinsider.com, 2012) and its purpose is to show the infiltration and mass usage of Facebook to nearly every place on earth there is internet access and the connections between its users.

As a result of such massive popularity, the issue of privacy on Facebook has received widespread public notice. According to latest studies almost 13 million users said that they had never set or didn't know about Facebook's privacy tools (Rosa Golijan, 2012). This is a very startling finding taking into consideration that Facebook is profoundly the biggest player in the field of SNS. Facebook has been openly criticized for targeted advertising through correlating data provided by its users and granting unauthorized access to personal data through third party applications even if the user chooses not to use them. In addition it is believed that Facebook sells data to third parties for profit (Drew Guarini, The Huffington Post, 2013). It is also accused of tracking its users' online activity even when

they are logged off (Olivia Solon, Wired UK, 2011). The last and most recent blow to date (2013) in Facebook's trust with its users came after reports suggested that the company granted the NSA access to its users data (Fiegerman, Mashable, 2013).

4.1 Facebook – The web 2.0 phenomenon

With the emergence of Web 2.0 web sites evolved from being static to dynamic. Originally data was posted on the web site and the user simply viewed or downloaded the content. Increasingly, users in order to see the content of a web site were supposed to interact both with the site and with other users. Not all SNSs could keep pace to the swift change and some got left behind but Facebook took a leading role and became a pioneer as far as SNS are concerned. Facebook transitioned from being static isolated data storage to a dynamic user-driven and participatory site constantly expanding at the expense of privacy.

At first (2004-2006), people used Facebook as an advanced personal blog where they could add personal information, view other users' profile pages, communicate and comment on shared material. When the first major changes took place (2006), sharing information gradually became easier, faster and more direct making users able to literally share every second of their lives. Then, as Facebook grew in fan base, there were others who wanted to get benefited from this directness of interaction with such an amount of people and Facebook realized it could expand its services. As a consequence, Facebook allowed to companies, celebrities, professionals and individuals to promote and even advertise their products and services as there had been significant progress in data mining techniques and targeted advertising had been flourishing.

Those changes accompanied by the evolution in the concept of sharing and disseminating data converted users to data providers for businesses. Personal information as well as browsing habits and interests were (and still are) of enormous commercial value to advertisers who used all this data for tailor marketing and advertising. Facebook took advantage of the continuous flow of information and allowed third parties to gather it through granting more access rights to them.

Facebook knew that the un-preceded success it received relied heavily on the number of users that visited the site and shared data on a daily basis. Therefore, it should keep users' trust and confidence, that it acts on their service, unharmed. It is true that it started in that direction, offering comprehensive and clear policies towards data collection and processing along with sophisticated privacy settings. However some choices (discussed below) that were followed by drastic changes in those settings would test users' trust in company's intentions and praxis eventually leading many of its users to pull the plug on their Facebook profiles as studies proved (Woollaston, Mail Online, 2013).

4.2 Facebook services

4.2.1 Facebook 1.0.1 – creating a profile

New users of Facebook must create a profile and they begin doing this during the registration process. A message on the Welcome page emphasizes Facebook's networking potential – "Facebook helps you connect and share with the people in your life" – highlighting scope to keep up with family and friends, share photos and videos, and reconnect with old classmates. Users are asked to fill in the minimum information needed to set up your profile – name, date of birth, password and e-mail address.

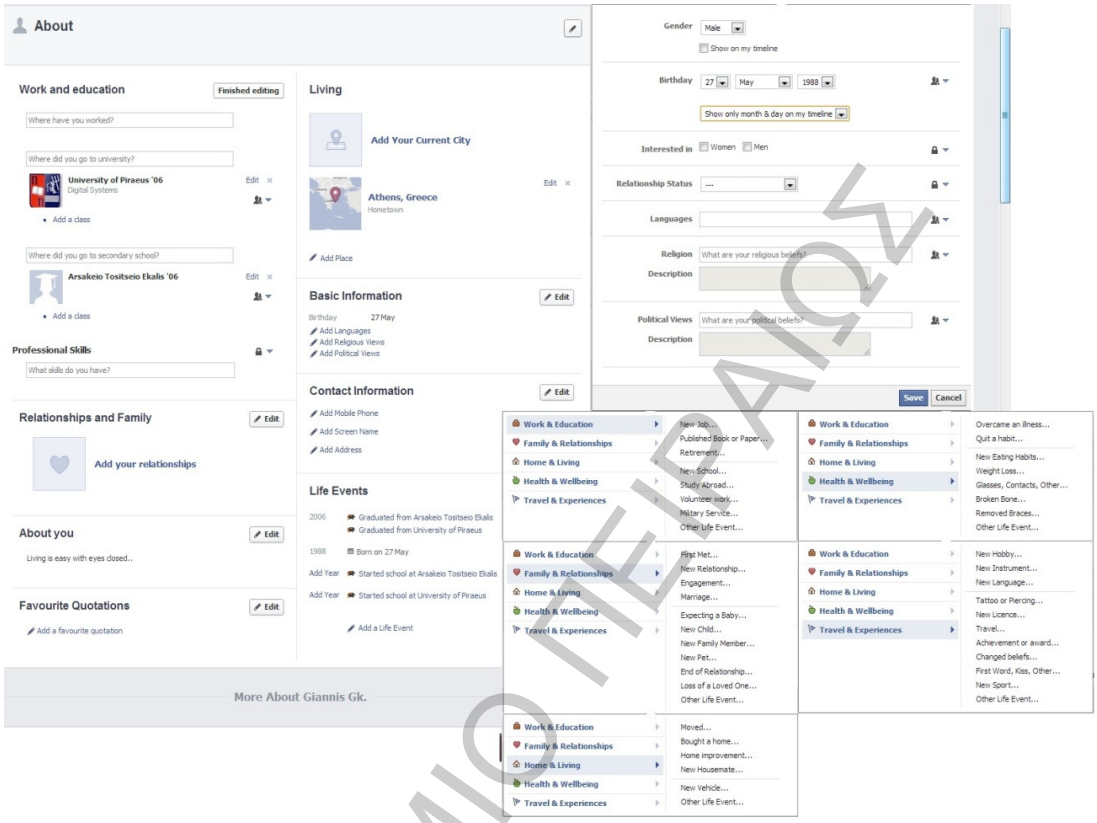
Facebook's Terms of use for individuals require you not to "create an account for anyone other than yourself without permission." However, the system does not validate a registrant's name, age or contact details when setting up a new user account. To this point however it is worth mentioning that it can have both positive and negative effects towards privacy. On one hand it ensures privacy as one can choose not to provide its full name and birthday information and retain to a certain extent his anonymity, on the other hand it facilitates the use of fake profiles with the risks to privacy and security that were mentioned earlier. Users automatically accept Facebook's Terms of use and Privacy policy by clicking 'Sign Up' on the Welcome page – there is no separate tick box to indicate that you have read and understood these conditions as in many other occasions.

After signing up, the standard process of email confirmation follows and Facebook asks for email address confirmation by picking up a message from the provided email

account and following the link it contains. When users complete this process registration is over and they are free to edit their profile, find new friends and start sharing.

4.2.2 Editing a profile

Profile details comprise what an individual is willing to enter into the system and make public and viewable by others. Aside from name and e-mail address, all other data fields on Facebook may be left blank, so the creation of a minimal Facebook profile is possible but that is rarely the case. It is important to keep in mind that any information posted beyond these basic fields is posted by the will of the end user. A typical Facebook user profile frequently includes large amounts of personal, and even, in the terminology of the European Data Protection Directive (DPD) (article 8 DPD), "sensitive" personal data. Sensitive personal data is defined in the DPD as "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning health or sex life*" and it states that whenever it is to be processed it should be done with extreme caution. A closer look to Facebook profiles is all it takes to realize that they contain almost every category of the data deemed "sensitive" by the DPD. Sexual details (looking for man/woman/both), religious beliefs (Jewish/Christian/atheist), political views (liberal/conservative) and medical history (undergone surgery/overcame illness) hang in plain sight as the following screenshot of a Facebook profile "About me" section suggests.



In other words, "About me" section in a Facebook profile is like one's own identification card inside the network with much personal identifiable information gathered in one place (name, address, telephone number). Personally identifiable information refers to "*information that can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual*" (Data protection act, 1998). Studies have proved that people hold a wrong perception about internet which they perceive as a private space where they can share secrets and personal stuff eventually leading them to share personal and even sensitive data (Levin, Abril, 2009), (Edwards & Brown, 2009). Users in this section can share a multitude of different types of data including:

- **Work and education:** where users are prompted to fill the name of their work or institution along with the year, the people they were with and the duration and subject of the course in case of studies.

- **Relationships and family:** where users are asked to state their relationship status and list their entire family along with 27 possible relations.
- **About you & favorite quotations:** a section that seems to be the most safe to fill without worrying if someone's watching.
- **Living:** where users state their current location and their hometown and a miniature map helps to avoid misunderstandings.
- **Basic information:** Those have to do with your birthday, languages spoken, sexual orientation, religion and political beliefs.
- **Contact information:** generally all the information that someone needs, if he was to contact you in real life, gathered in this section. Emails mobile and work/home phones along with address and zip codes compromise the user's privacy in lots of ways.
- **Life events:** one of the most privacy endangering elements that came along with Facebook timeline feature in 2011. Not only all the above are included in this section in full detail (date-to-date, photos attached, people tagged) but also 2 new categories added one named **travel and experiences** and the other **health and wellbeing** where someone is free to share his medical record with all his contacts.

In addition, a photo is required to make the profile seem legitimate amongst the Facebook community -a photo that states the place where it was taken along with the time and date- because none would want to interact with someone who's hiding his face. Moreover, Facebook offers users the possibility to also share videos, songs and articles and make lists of hobbies and interests like favorite books, movies and TV-shows. In 2010, Facebook added a new feature titled 'Places', this enables a user to see where their friends are in addition to sharing their own location. Users can communicate with others by using profile "walls" or private message features. Writing something to others wall is normally visible to everybody who can see this profile and information in it. Users also can comment on photos, videos or other posted elements. With using "status updates" users can also tell the others what they are doing, where they are, and so on. Last but not least, Facebook has

its own platform in order to develop applications that can be connected to profiles in order to enhance one's experience (or breach one's privacy).

Apart from that, Facebook responds to the need of people to belong in communities with same interests, political views and religious beliefs with the ability to socialize in groups with open or closed entrance. Furthermore, with Facebook pages the opportunity to advertise products or businesses is offered and people state whether they "like" them or not.

Taking all the above into account, Facebook has access to an immense amount about its users. Subsequently, a fully filled-out profile contains about 35 pieces of personal identifiable information. If added into the equation the connections that a user makes (friends, groups, likes) then, "*by the time you are done filling out your profile, Facebook has a reasonably comprehensive snapshot both of who you are and of who you know*" as James Grimmelmann writes (Grimmelmann, 2009). One doesn't have to be an expert in order to make the basic assumptions for the user just by watching his profile. Wall posts can contain information about both the poster and the postee, location services reveal users' current location and places they like to visit while tags in photos documents not only what each user looks like but also reasonable inferences such as the place and the kind of relationship between the users (Solove, 2004). Settings that can help users protect their privacy will be reviewed next.

4.3 The evolution of Facebook's privacy policy

Examining Facebook's privacy settings since its incorporation (2004) it is easily understandable that Facebook has undergone a tremendous transformation, from being a private space where users communicated with groups of their choice, to an open network where data is available to a much wider audience. As Facebook's core user base started growing, the privacy settings were getting less and less private and users were having limited control over their data in exchange for profits from selling its users' data to businesses and advertisers. For argument's sake, parts of Facebook's privacy policies over the years are presented:

- Facebook privacy policy 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 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 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 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 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."*

- Facebook privacy policy 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."*

- Current Facebook privacy policy as of 2012: *"we receive a number of different types of information about you, including registration information (when you sign up for Facebook, you are required to provide your name, email address, birthday and gender), information you choose to share (name, profile picture, networks, username, user ID are treated just like information you choose to make public), we receive information about you from your friends (such as when they tag you in a photo or at a location or add you to a group), we may also receive information about you from the games, applications and websites you use, but only when you have given the permission. As a general rule you should assume that if you do not see a sharing icon, the information will be publicly available. When others share information about you they can also choose to make it public."*

Each set of changes was followed by user backlash as levels of privacy were gradually decreasing. Protest groups were formed and users discussed their concerns via status messages hoping to be heard by the proper audience. First change came on September 5, 2006 when Facebook unveiled two new features: "news feed" and "mini feed". These changes were followed by sizable public outcries for loss of privacy because all activities of a user would be gathered and posted on his profile as well as broadcasted to all of his friends. After considering these complaints Facebook offered its users the possibility to choose whether or not any activity would be visible.

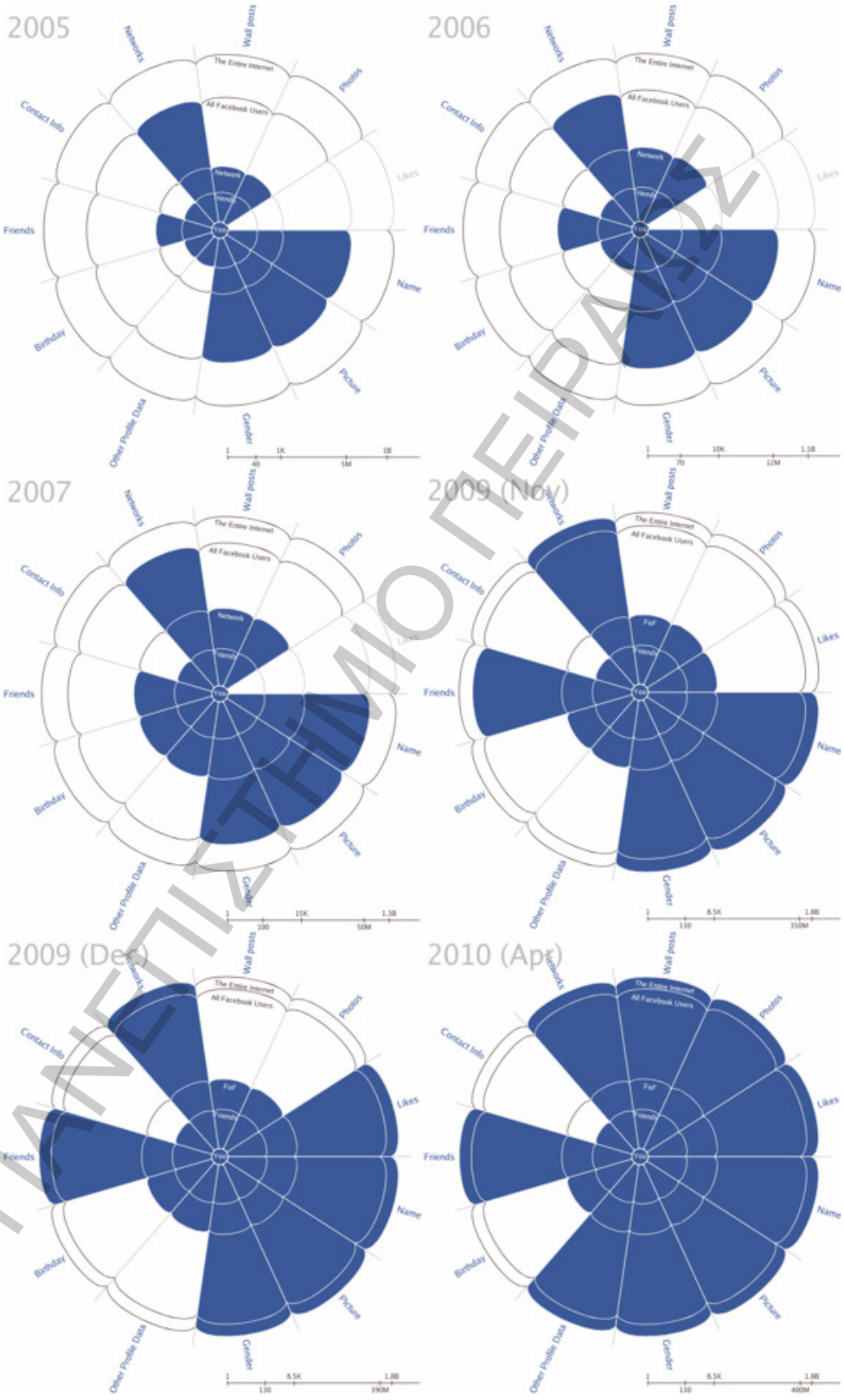
Afterwards, on November 6, 2007 Facebook launched its "Beacon" program making its first step towards the broader web and hoping to revolutionize advertising by posting updates to his users profiles whenever they performed any action within its partner sites. The privacy concerns raised and the objection of users against this direct sharing of details, concerning their actions on the web, led Facebook to initially change beacon program from opt-out (user had to unregister from the service) to opt-in (users could choose if their information would be posted) and eventually shut it down due to lawsuits filed against Facebook and its partner sites. This unfortunate (for Facebook) turn of events didn't stop the company from pushing to make more information public.

In February 2009, Facebook made unannounced changes to its terms of service without anyone noticing until several weeks later. These changes allowed gave Facebook full control and ownership over users' data even if users deactivated their accounts. This time it took Facebook only 3 days to revoke these changes and revert back to its old terms of service. It also asked for propositions regarding the new privacy settings by its users and for this move it received praise by the community.

However, few months later (fall 2009), Facebook presented the new privacy policy that was characterized as "Facebook's great betrayal" (Gawker.com, 2009) or "evil and outrageous". All information, since the day each user logged in Facebook, overnight and without any warning became public regardless that it might have been kept private all these years by the owner. Facebook claimed that these settings would enhance privacy but no user was happy with this particular change. Later on Facebook would introduce its "timeline" feature facilitating the search of old posts even more. During this transition even Zuckerberg's private photos were visible to all. Needless to say he altered his settings quite swiftly.

In April (2010), the site started granting access to user data to third party applications. It was noted that this access would last for a day (24 hours) but was later discovered that until users uninstalled these apps, data would be stored indefinitely. Instant personalization was also launched allowing certain websites to personalize their sites with data provided from users' accounts. Any information which was publicly available could be used to make the website more friendly and interesting to the user. As with beacon project, users were automatically enrolled but now can choose to disable it.

For better understanding of the changes that have occurred over the years the following picture is provided. Each piece of the pie diagram represents the data shared and the audience, which is illustrated with the blue color, gets more public as it moves to the perimeter of the circle.



Just by giving a glance at the infographic (Facebook's Privacy Erosion Strategy Virtualized, www.theusrus.de, 2012) it is clear that with each update more personal data becomes available to a wider audience. It is quite disturbing for those who endorse privacy to witness such drastic turn from private to public. Note that every time these settings were updated, they were set to default (meaning "public") without informing the user who might had configured them.

Summarizing, there seems to be an ongoing conflict between users who ask for control over their own data and Facebook which constantly keeps ignoring these cries for privacy. On the contrary, the two most crucial things to keep in mind are that Facebook is constantly performing unannounced changes on its privacy policy and settings without informing until it's too late its members and that deliberately conceals how they really affect privacy. It was pretty obvious since the very first changes occurred that Facebook didn't have the privacy interests of its members as first priority when setting new policies. That can be explained as Facebook's income derives, at least partly if not entirely, from data disclosed by users and so its financial incentive is arguably to maximize disclosure and minimize privacy (The Guardian, 2007).

4.4 Users attitude towards privacy policies

Generally speaking internet users don't read privacy policies and Facebook users are no exception to that rule. A survey conducted back in 2001 found out that only 3% of people claimed to read privacy policies carefully "most of the time" (Harris Interactive, 2001), and a later study in 2007 raised the proportion to 31% (Zogby Interactive, 2007). Those users who do read privacy policies generally don't understand them. Studies showed that although users claimed to care about privacy and to look to see whether sites had privacy policies the vast majority of them were badly misinformed about what those policies actually said (Turow, 2003). A 2006 (Acquisti & Gross, 2006) survey on Facebook users showed that 77% of them had never read its privacy policy and that nearly all of them had wrong beliefs about how Facebook collected and shared personal information. Some also claimed to have read the policy but were unable to understand the level of privacy it offered.

If users did read Facebook's privacy policy closely and if they could understand it they would know that it doesn't restrict unauthorized access and it contradicts itself given the opportunity. Facebook has a terrible reputation when it comes to privacy (Vallance, BBC News, 2008), (Schneier, Epic.org). In short, users don't read it, don't understand it, don't rely on it and certainly aren't protected by it.

4.5 Facebook privacy policy – an overview

This part of the thesis doesn't intent to analyze in depth and from all aspects the terms of use. Its goal is to provide an overview of what should be expected from the users concerning their data prior to joining and highlight the significant role that advertising plays in Facebook's policy.

In a previous section, it was mentioned that all that is needed to join Facebook is to be more than 13 years old and have a valid email account. In fact one more thing is needed and that is a formal indication of consent to the privacy policy. Unfortunately the complexity and length of the policy makes it unlikely that users read it in detail. Bruce Schneier offered an interesting yet predictive opinion to the matter by stating that "*Facebook can change the rules whenever it wants. Its privacy policy is 2.800 words long and ends with a notice that it can change at any time. How many members ever read that policy, let alone read it regularly and check for changes? Facebook can sell the data to advertisers, marketers and data brokers. It can allow the police to search its databases upon request. It can add new features that change who can access that personal data and how*" (Schneier, 2006).

To begin with, although it is mentioned that users should be informed about reasons and ways of collecting data and that Facebook encourages them to do so, the data use policy is hard to notice and find in the privacy menu (there is no "I agree" button to tick). It is also stated that user has control over his data, choosing which data to disclose and by configuring privacy settings selecting the preferable audience. However these settings refer to data shared between users and the issue of sharing users' data with advertisers is ignored. Since 2011 there are no privacy settings that prohibit access to information for advertisers except some minor settings relating to "social advertising". In simple words this means that users are never asked whether they agree or not to targeted advertising and so they have to

take it for granted. Targeted advertising is always activated and there is no opt-in or opt-out choice. Users are not asked if they want their data to be sold to advertisers therefore actual user consent never occurs.

Facebook admits it aggregates data like browser history, IP address and installs a cookie that helps advertisers track users' activity through the internet and collect data about their behavior. An opt-out option is deeply hidden in the privacy policy and is not visible in the normal settings making it highly unlikely that users eventually opt-out. This shows that Facebook clearly values profit over privacy.

Users are on the other hand encouraged to provide as much valid information as possible and not use any pseudonyms or nicknames. Anonymity is nearly impossible to get because the IP together with the email address can reveal the digital identity of a user. Complete account deletion is impossible and it is noted that some information will *"persist in backup copies for a reasonable period of time"* and that *"information of you provided by other users along with your name and your messages will be still visible"*. Unsurprisingly, (as users and their data are key components to Facebook's structure) Facebook tries convincing you to rethink about leaving with pictures of your friends who, the site warns, will "miss you" if you deactivate your account. Users must delete all information posted by them one by one and ask from other users to do the same with posts that include them if they want complete invisibility for their data. Even if they did this, which would take much time, some data would remain in a database. Users are also informed of the possibility of illicit actions performed inside the Facebook from other users such as replication of data and unauthorized re-sharing. Additionally, Facebook gathers email addresses of people that have no interest in joining the network. This happens when newly registered users give permission to Facebook to scan their email accounts and find contacts that are already using Facebook in order to connect them.

As far as apps are concerned users can choose which of their data will be passed on to advertisers. Even if a user chooses not to disclose any information or not use apps at all data will leak through his friends provided that his friend is using the service. Data collection by application third parties will take place once a day for enhancing the

application service as it is stated and Facebook bears no responsibility to what happens to the data collected by third parties.

In conclusion, Facebook seems to be gathering much more data than the user even considers. Facebook's privacy policy puts capital interests first and diminishes user and data privacy. It is long and written in a complex language in order to cover up its real purposes which are the economic surveillance of its users and the commodification (or "sharing" in Facebook's terms) of user data for targeted advertisement. Additionally, Facebook actually never asks for users to give their consent before selling their data to advertisers but coerces them into having to accept the policy in order to use the platform and its services. Facebook perpetually hides opt-out options, like for instance from cookie-based advertising and provides a minimum of advertising privacy options in its menu. Facebook also collects and commodifies data about user behavior on other websites. As if these were not enough, terms and policies can be subjected to any changes without informing the users who will primarily be affected. After considering all of the above it is reasonable to assume that Facebook acts more like an advertising platform that wants to store and sell as much user data as possible in order to maximize its profits.

4.6 Default privacy settings

"We're building a Web where the default is social." - Mark Zuckerberg

When referring to default privacy settings it would be reasonable to assume that these would be the means to protect data and privacy. On the contrary these settings expose more data than they protect. In particular, privacy settings by default reveal as much data as possible and considering the fact that the majority of the users skip the process of configuring their settings either because they "trust" the provider or because they simply don't realize to what extent their personal information is threatened, privacy is clearly diminished. As Facebook profits by having users' data accessible to the widest audience, the burden for securing privacy falls off to the users. In this section we will review firstly how privacy by default should work and then how it actually works.

4.6.1 Privacy by default

Privacy by default is defined by DPD as *The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.*

Additionally, Weiss states that on the traditional Web, privacy is maintained by limiting data collection, hiding users' identities and restricting access to authorized parties only, while the reality of OSNs is that data and identity become closely linked, and are often visible to large groups of people. It becomes harder for a user to monitor and control his personal information, as more of it becomes available online. Together, this makes managing information and privacy a lot more difficult. The default privacy settings should protect users' personal information and not expose it. In particular, this means that setting by default profiles to "private" (or to a user-approved contact list) would reduce unwanted exposure and leakage of personal and private information. The user should be able to choose less private options being responsible for anything bad would happen. Users shall also be able to report inappropriate behavior of another user so as to help the providers in deactivating users who act improperly.

Providers should include mechanisms for reporting inappropriate behavior, which shall be easily accessible to the users at all times with an understandable procedure of using them. Users should be provided with the information they need to make an effective report and, where appropriate, an indication of how reports are typically handled shall be included (European Social Networking Task Force, 2009). SNS providers should also provide users technological solutions for protecting their private information and specific role as data controllers to control themselves how and to what extent their data will be disseminated. Social networks should provide privacy awareness methods for their users and offer them a number of tools so as to be able to form their own privacy policy always ensuring that it is based on the respective legal and regulatory framework. Social network service providers

must provide the tools for the handling of every piece of private user information, as the only responsible for the private data set is the respective data subject.

4.6.2 Users' approach towards privacy

Social networks have become a projection of real life for millions of users who build explicit networks that represent their social relationships and share a vast amount of personal information. The potential privacy risks of these behaviors are in most cases ignored or underestimated so the assumption that users are lacking in awareness and in experience would be fair to make (Hargittai & boyd, 2010). In addition to that, the poorly designed privacy management settings add another significant factor to the problem of users' privacy on SNS. Due to the lack of awareness and experience many users find the privacy controls too complex to process, understand and set according to their privacy needs and so they may either set them incorrectly or ignore them and settle for sub-optimal privacy protection.

Gross and Acquisti (Gross & Acquisti, 2009) show in their research, that most of the users don't change the default privacy settings that are provided by the SNS, while sharing a large amount of data on their profile. Another study performed by Tufecki (Tufecki, 2008) concludes that even though privacy-oriented users are more reluctant to join SNS once they do join they disclose quite a lot of information a situation that had been previously characterized by Barnes as a "privacy paradox" (Barnes, 2006). Users are also unaware of the audience that their data received along with trouble configuring the settings offered as recent research proved (Liu et al., 2011).

Other research has offered several explanations for this underutilization of privacy options (Dwyer, 2007), including poor interface design and permissive default settings (Gross & Acquisti, 2005), social conformance (Govani & Pashley, 2007) and inherent trust in the online community (Acquisti & Gross, 2006), (boyd & Heer, 2006), (Gross & Acquisti, 2005).

4.6.3 User information

Concerning data provided by the user, even though nearly all data is visible to the entire internet by default, with only contact information being kept for friends, users can take matters into their own hands. So unless the user wants to share everything with everyone he has the ability to manually configure the audience of his posts. Facebook offers the possibility to choose between 5 desired audiences, public, friends of friends, friends only, only me and custom. As already mentioned, default setting or recommended is "public" meaning data is accessible from 1.1 billion users. "Friends of friends" is exactly what the title reads, where data is viewable by users who might not have direct access to one's profile, while "friends only" makes the data available only to those the user has confirmed as his "friends". "Only me" makes the profile rather dull (speaking from the perspective of a social network fan) as information posted is viewable only by the owner of the profile. Lastly, by custom, a user can manually choose which of his contacts can see each post. These options are available for each piece of content a user wishes to share and for each field that contains personally identifiable information.

If privacy was only about the data that the user decides to provide, then Facebook would have done a rather good job in allowing its users to decide for their data visibility. But implications exist when talking about data that comes from other users. Typically when a user wants to publish information that involves other users he has to ask for their consent in advance (according to the European data protection legislation). This would cause a great problem to the concept of rapid and instant sharing of activities in SNSs due to the complexity that this request adds. This should have been regulated from Facebook in the first place of at least offered through privacy settings. Instead of that a user can un-tag (unlink a photo from his profile) himself only after the photograph is uploaded and cannot remove the picture. By default this tag review isn't available and users freely include others in their posts. The same settings apply for tags in places.

In addition, by default, anyone can search for a user both inside the Facebook's premises and outside using the search engines (Google, MSN Live, Yahoo). However, the user can choose to opt out of the public search listings. Aforesaid, Facebook "timeline" revealed every action the user had performed over the years which was by default available

to all. Surprisingly, when trying to limit this audience from “everyone” to just “friends” there are signs and warnings by Facebook advising of not doing so.

4.6.4 Apps and ads

Facebook introduced its application platform back in 2007 allowing third party developers to create applications that would enhance social networking experience. There is a wide variety of apps to chose from mainly consisting of games and quizzes. Facebook applications have received significant attention due to reports that they leak data (names, Ids, contacts) to dozens of advertising and internet tracking companies. This is very disturbing considering that tens of millions of Facebook’s members use these apps and even those who chose the strictest privacy settings seem to be affected. When a user tries to use an application he is informed of the data that the application requires in order to grant access to the user. Apps have access to any information the user chooses to make public along with basic info which is always publicly available. Moreover, apps access the same information for all of a user’s friends regardless if the others are using them as well. The problem extents as users have the impression that they’re interacting with Facebook due to the fact that they use the applications within the boundaries of the network. In fact, they could be sharing with anyone hiding behind the legitimate development of apps. However there is the option to opt out from the application platform but then usage of any application is permitted.

Another feature that was announced back in 2007 along with applications was Facebook’s social ads. “An entirely new advertising solution for Facebook”, it was called and displayed relevant advertisements related to actions and interests of users. Although there were assurances that only fellow contacts (and not the advertisers) would see who was checking advertisements and no personal data would be disclosed to advertisers, reports of targeted advertisements began to flourish.

Advertisers not only receive data from Facebook for targeting advertising, they also use small programs, so-called cookies, to collect data about user behavior. Facebook provides an opt-out option from this cookie setting that is not visible in the normal privacy settings, but deeply hidden in the privacy policy with a link to a webpage, where users can deactivate cookie usage by 66 advertising networks (as of January 19, 2011). The fact that

this link is hard to find makes it unlikely that users will actually opt-out. This reflects the attitude of many commercial websites towards privacy protection mechanisms as being bad for business. It also shows that Facebook values profit much higher than user privacy, which explains the attempt to make the usability for opting-out of cookie use for targeted advertising as complex as possible.

Facebook reduces the privacy issue to visibility of information to other users. In the privacy settings, users can only select which information to show or not to show to other users, whereas they cannot select which data not to show to advertisers. Advertising is not part of the privacy menu and is therefore not considered as a privacy issue by Facebook. The few available advertising settings (opt-out of social advertising, use of pictures and name of users for advertising) are a submenu of the "account settings". Targeted advertising is automatically activated and cannot be deactivated in the account- and privacy-settings, which shows that Facebook is an advertising- and economic surveillance-machine that wants to store, assess, and sell as much user data as possible in order to maximize its profits.

Concluding, Facebook privacy settings (at least default) are not in any way privacy enhancing. They are hard to understand, hard to find and in many cases negate one another. It requires time to fully configure them and full understanding of the usage and importance of each setting. Unfortunately, as personal information is treated as profit asset the possibility of getting more privacy-oriented settings in the future seems unlikely.

4.6.5 Application of the Data Protection Directive to SNS and search engines

European Union has set high standards towards the protection and processing of users' personal data along with strict obligation to entities that process such data. Therefore a major issue arises concerning the EU citizens' privacy rights and the applicability of the European Data Protection Framework on SNS providers and search engines established outside the EU. Article 29 Data Protection Working Party suggests that the provisions of the Data Protection Directive apply to the providers even if they are located outside the EU (Article 29 Data Protection Working Party, 2009) and more specifically if they have establishments in the territory of an EU Member state or they use equipment situated on an EU Member State (Article 29 Data Protection Working Party, 2008).

The DPD defines two basic categories of parties, which are relevant to be identified in the context of social network services. There is the data subject who is the individual to whom the personal data is related and the data controller who is the individual who is responsible for the purpose and means of the processing of personal data. In other words, it means that this individual decides which data is collected and processed as well as the means for the processing. In addition the DPD suggests specific obligations for the controllers regarding the processing of personal data, the respect of the rights of the users and their responsibility in case of breach of law. It also states that the providers of the SNS are the ones responsible for the means of processing as they provide the platform and the tools for user management (registration/deletion of accounts). Moreover, the providers of the SNS also determine which data will be used for marketing and advertising purposes. Therefore it is reasonable to assume that they are regarded as data controllers.

Users on the other hand are more difficult to be characterized as data controllers. Users of SNS in general choose whether they want to disclose information or not with other users but also they share information of other individuals. They may also use specific application on a social network in order to reveal information. Alsenoy suggested in his research that users can be described as data controllers as they choose what information they want to share and they initiate processing operations (Alsenoy et al., 2009). The DPD provides the "household exemption" and refers to processing of data performed in the course of a purely personal or household activity. As publication on the internet makes data accessible to an indefinite number of people this exemption can't apply in the case of social network users (Wong, 2008). The article 29 Working Party considered the status of a user account (public or private) in order to classify him as data controller which is a rather arbitrary criterion (Alsenoy et al., 2009).

Concerning the use of cookies from SNS and search engines that were mentioned earlier, according to the Article 29 Working Party the installation of cookies to the terminal equipment of European users form a provider established outside the EU is considered as use of equipment and invokes the European data protection legislation (Kosta et al., 2009). The collection of personal data by means of cookies enables the controller to link up all information he has collected during previous sessions with information he collects during subsequent sessions. In this way, it is possible to create quite detailed user profiles. The use

of cookies, which track activity on a computer's Internet browser, has been standard practice of various search engines. Information is stored about the end-user and enables in this way a relationship between the server and end-user. Of course, cookies don't always necessarily identify a person by name, which is the case for instance when more people use the same web browser to make a search query without subscribing to the service (Glasner, Wired.com, 2005). This approach of the Article 29 Working Party to consider the use of cookies as use of equipment has however been criticized as "unconvincing", especially by providers established outside the EU (Kosta et al., 2009). It has also been characterized as "regulatory overreaching" in an online environment, in the sense of "a situation in which rules are expressed so generally and non-discriminatingly that they apply *prima facie* to a large range of activities without having much of a realistic chance of being enforced" (Kosta et al., 2009). The position of the Article 29 Working Party can thus be questioned or endorsed, according to the position one takes on this matter (Kuner, 2007).

4.7 Major Facebook privacy concerns

Social networks gather a range of information from users – from information users provide directly to the site, to information revealed when users interact with the site, to information gleaned from users' interaction with third parties. After considering the above, it should be understood that responsibility for loss of privacy isn't entirely up to the users but also to Facebook who is in a way luring users into over-sharing data under false promises. Disclosure of information and online popularity become interrelated into Facebook members' minds thus serving Facebook's and its partners' purposes. In this section, privacy concerns and data protection issues will be addressed.

4.7.1 User related privacy concerns

In many cases, privacy is breached not only from unregistered visitors but also from fellow SNS users. In the first case, this may be a deliberate act as a result of hacking or phishing while in the second, accidental due to mismanagement or neglect of privacy

settings by the user himself. As a result, privacy becomes compromised and serious problems and consequences can arise affecting all aspects of a user's life.

Facebook encourages its users to over share data while they falsely assume that this information will be kept restricted from wider audience and will be visible only to friends. Disclosure of information like full name, maiden name, complete home address, email address, home and cell phone number, relationship status can cause a huge problem as the more information there is available the easier it is for a malicious user to use it in his favor to serve his purpose. Maiden name or high school information is part of the security questions posed to the user who forgets his password (Brad Dinerman, 2011). This information is also available in the profile section and can be used along with the email address to help malicious users verify themselves as legitimate ones. In addition, disclosure of contact and residential information aid in the expansion of threats like identity theft and cyber bullying.

Sometimes a user would like to hide information from a specific contact such as an employer (Jordan Valinsky, The Daily Dot, 2013) or his parents but due to lack of awareness of his share visibility he ends up sharing the wrong information with the wrong audience. Facebook can be damaging for prospective employees looking for work, as it offers revealing information about a candidate's true colors. Several profiles often contain awkward and embarrassing information that job seekers would not want their future managers to know about themselves (Neetzan Zimmerman, Gawker). Moreover, there have been many instances where personal status updates or posts have hurt or damaged a company's reputation, thus seeing many employees lose their jobs over mindless updates that they didn't think twice about. A fine example of one employee who damaged her reputation after she wasn't awarded a promotion: *"This place is a joke!!! I wonder if I passed up a good opportunity by being at this place. I absolutely hate fake and lazy people!!! Ugh, the ones who actually work are the ones to blame???"* It wasn't long before her boss received notice as she was friends with several of her coworkers (Jordan Valinsky, The Daily Dot, 2013). Another example of "bad" sharing comes from location based services offered in Facebook commonly known as "check in" where a user states the place he is at the actual moment but more importantly he shouts that he isn't at home. This is a

perfect opportunity for a malicious user to take advantage of such knowledge and rob someone's house while he is out.

Even if a user is careful in controlling what information he posts to a SNS he has limited control over what other users post in the same SNS. Often messages and status updates contain information about multiple SNS users, or even non-users. This can occur when another user posts information about you which you don't want to be shared or when information disclosed privately to another user is made available to a larger audience due to his settings. Another example of an employee who lost his job due to getting caught red handed is the Kevin Colvin incident. He asked his supervisor for an absence leave claiming he had some serious family issues. His goal was to skip job and attend a costumes party in New York where a friend of his uploaded in his profile a photo of him wearing a fairy's costume. His supervisor was able to see the photo and commented "cool wand". Needless to say he was fired the same day.

4.7.2 Facebook related privacy concerns

A completely different type of privacy threat involves the relationship between Facebook and the user and in particular the trust that the user puts in Facebook. Facebook and third parties collect and process user data and the informational practices used could be potentially considered as privacy issues. This is a rather grey area as little is specified about process followed, purpose of data acquisition and whether user consent is adequate and intentional.

- **Collection and storage of information** refers to the acquisition and retention of users' personal information by Facebook and the third party applications.
    - **Data collection by Facebook** uses, in a way, interrogation and surveillance methods in order to collect and store data from its users. Interrogation refers to the direct acquisition of data from users by asking questions relevant to the profile and personal information. Profile information (name, email, gender, birthday, location) is obligatory to provide in order to become member on

Facebook while personal information (relationship status, political religious views, interests, work history and education background) is entirely up to the user to disclose. In all boxes that information is required lays a question tempting the user to truthfully answer. "*Where have you worked, where did you go to university, where are you and with who, what's on your mind"* are only some of the questions that seek for an answer. On the other hand, there is also the indirect way of acquiring data by tracking users' actions online even outside of Facebook's boundaries. This is achieved with cookies installed to track down any action performed on fellow web sites, browsing history, IP address and location information when connected through mobile devices.

- **Data retention issues**. When posting information to Facebook it is often impossible or very difficult to remove that information, for several reasons. Facebook, for example, does not provide users with the means to delete their profile, and has actively blocked third-party software that attempts to remedy this (Paul MacNamara, NetworkWorld, 2010). This is because the capital of an SNS often lies in the number of users, and data sales are sometimes part of the revenue. Facebook would like to store content forever (cwalters, Consumerist, 2009). Secondly, information (especially in a social context) tends to be replicated. People may spread information or multi-media and even store it locally and re-upload it at a later time. Finally, information that is apparently erased may still reside elsewhere on the SNS, for example in backups, to be found by others. Similarly, a resource may be disabled or seemingly deleted, but references to it (thumbnails, messages on friends' pages etc.) can remain visible to the outside world (Ryan Tate, Lifehacker, 2009).
- **Data collection and storage by third parties**. Privacy issues caused by third parties apps concern apps from friends and pre-approved third parties. In the first case the real issue is the ability apps have to access all information visible to a user, including his friends' personal information, even if his friends never granted access to the application. Another privacy

concern is the pre-allowed access to public information, Facebook has granted in advance on these applications.

- **Processing and use of information** involves the editing and handling of the collected data. Processing and use of information is held by the same two parties: Facebook and third parties.
    - **Processing and use by Facebook.** Users understand that their data is being collected and used by Facebook as it suggests them contacts, based on location, mutual friends and education/work history. It also suggests them products that their friends use based on purchases or likes on the product's page. It isn't hard to understand that users loose the control they have over their data from the moment Facebook gets its hands on it. No opting out or consent of any kind is asked by them for processing and using their data.
    - **Processing and use by third parties** mainly refers to targeted advertising. Facebook and third parties gather information from users in order to craft advertisements that best suit the consumers. Interests, purchase and browsing history and in certain occasions life events are some of the personal information being used inappropriately and for different purposes than the initially agreed ones.

4.7.2.1 Third party applications on social network

Within the context of social networking, "third-party applications" are programs that interact with a social network without actually being part of that social network. These applications take many forms but some typical and popular forms include:

- Games to play with contacts
- Online polls or quizzes
- Software that allows users to post to a social media profile via a cellular phone or web application

Some social networks allow program developers to access their platforms in order to create these applications. This makes the social network more attractive to users by facilitating the development of new and creative methods of interacting with contacts and the network.

To make these applications useful, social networks may allow developers automatic access to public information of users. In addition to public information, third-party applications may access some private information. A user may grant a third-party application access to his or her profile without realizing the extent of the permissions being granted. Users may also mistakenly assume that third-party applications are held to the same standards as the primary social network. There are also "rogue" applications which do not follow the policies and terms agreed.

Some facts to keep in mind when considering using third-party applications:

- They may not be covered by the social network's privacy policy.
- They may not be guaranteed to be secure.
- Most social networks do not take responsibility for the third-party applications that interact with their sites.
- They may gain access to more information than is necessary to perform their functions.
- Sometimes applications are designed only to gather information about users
- They may contain malware designed to attack the user's computer.
- Third-party developers may report users' actions back to the social networking platform.
- A social network may have agreements with certain websites and applications that allow them access to public information of all users of the social network.

Third-party applications typically can access information that:

- Is considered public without explicit consent from the user.
- Is considered private when a user grants the application permission.

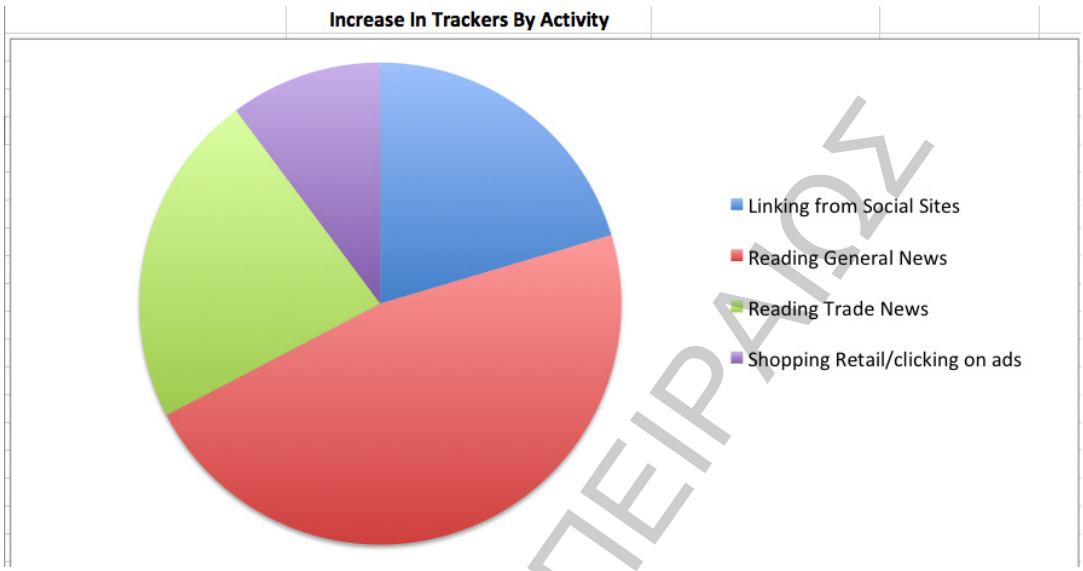
In some instances, once they have received permission from a primary user, the third-party applications may also gain access to the personal information of users' contacts without those contacts granting explicit permission. As a general rule, use caution when using third party applications. Remember that it is difficult to control what information they are gathering, how they might use it and who they will share it with.

4.7.2.2 Facebook tracking through "likes" and cookies

Tracking and tracing users on the web is an old concept that allows content providers to "remember" preferences of users, such as language settings, next time they visit a website. When Facebook introduced instant personalization it allowed partner sites to implement famous "like" button on their own pages in order to attract more visitors. Facebook's goal (as it was announced) was to give users ways of discovering both new content and more common ground with people they are connected. However, even though presented as a useful business tool the button was found placing cookies and tracking users even when they did not press it.

Essentially this means that actions performed on these sites (listening to a song, watching a video, buying tickets) were instantly broadcasted to user's profile and Facebook never asked for permission to do so. More on that browsing behavior of individuals can be connected to user's Facebook account. Even if the user didn't have a Facebook account in the first place, when he decided to sign in that data would connect to the newly established profile page. Hopefully you can stop Facebook from knowing every site you visit by opting out and delete all cookies from your system. The result of all the above is that Facebook gains more data to sell and that advertisers can target users and their friends more easily and with greater results.

According to an experiment conducted from researches and published in Business Insider Facebook trackers have specific interests and in particular are interested in what users read on the web, what purchases they make and what they are linking from social media sites (Felix, Business Insider, 2012).



(http://tylert123.blogspot.gr/)

Summarizing, Facebook privacy policy clearly states that any information provided by the users may become publicly available. Concerns over privacy begin to rise whenever users share information whether or not they decide to configure privacy settings. Apart from the obvious problems that concur when users neglect privacy settings there are many more that derive from the fact that data is aggregated, stored and used in ways that are never clearly explained to the data owners and providers. Even more, users' consent isn't asked at once and it is indirectly acquired and questions remain whether or not users who grant access do it willingly and in full understanding. Users have few power over the actions that are performed followed their registration to the network. They do have a choice though. They can live by what they signed-up for therefore, allowing others to collect their information and use it, or they can choose to do nothing at all and not to use any of Facebook's services remaining silent and idle. An "All or nothing" approach to such a serious problem that is privacy and data protection is something few would have foreseen Facebook endorsing in its early days as *"the most private network"*.

5 Countermeasures

The existing research in privacy protecting technologies suggest that in order to protect user data from other users, awareness and proper tools for managing and enforcing access policies play a leading role (Carminati et al., 2007), (Leenes, 2010). However this doesn't work towards solving issues that involve un-trusted service providers. Obscuring and hiding sensitive data from the providers (Anderson et al., 2009), (Guha et al., 2008), (Tootoonchian et al., 2009) or removing them entirely from the picture (Buchegger & Datta, 2009), (Shakimov et al., 2009) are some approaches that have received notice and generally refer to common security techniques including anonymization, decentralization and encryption.

5.1 Privacy Enhancing Technologies

Privacy enhancing technologies (PETs) aim to reduce the risk of collision between privacy principles and legislation, to minimize the amount of personal data being held by other parties and to provide individuals with control over their information that is being held. The European commission defines PETs as "*a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system"* (COM(2007) 228 final).

PETs combine technologies that employ security measures such as encryption and access control mechanisms and blend them with other measures to enhance privacy. PETs provide users with the ability to hide their true identity through tools that offer anonymous or pseudonymous access to online services, control what personal information is processed, how it is processed and by whom through privacy audits and log files. Although there are much more mechanisms used to provide privacy there are some security controls that can cause implications on privacy, like monitoring tools.

Although PETs have been in use for several years their adaptation rate is low. PETs are not employed due to the fact that new PETs are constantly developed and the applicability and effectiveness of older ones can't be evaluated properly. Also, they lack user friendly interface and their use requires previous experience and knowledge with

Information and Communication Technology a factor that is very important considering there is limited user awareness towards privacy. Lastly, advances in privacy invasive technologies, like data mining and electronic devices with sensors and biometric identifiers, limit their effectiveness in enhancing and protecting personal data.

5.2 Privacy by design – Privacy by default

For many years there have been discussions concerning the future the regulatory framework around privacy in Europe. Several new tools, concepts and principles which had been less formally embedded into privacy legislation evolved into being central objectives. One of these principles is privacy by design.

In its first adoption, in 1995, PETs referred to application that would be embedded into privacy invasive systems. The need however to address privacy concerns in all stages of systems development along with the need for comprehensive solutions to privacy issues and not just technological add-ons was emphasized more and more by those who endorsed data privacy. Privacy by design is a principle for designing systems which requires respect for individual's privacy and protection of their data at all stages of a systems lifecycle, from early inception to development and disposition. According to the European commission, *"the use of PETs can help to design information and communication systems and services in a way that minimizes the collection and use of personal data and facilitates compliance with data protection rules. The use of PETs should result in making breaches of certain data protection rules more difficult and / or helping to detect them*" (European Commission, PETs, 2007).

The principle of privacy by design was originally developed by the Ontario privacy commissioner according to which *privacy and data protection is embedded throughout the entire life cycle of technologies, from the early stage to their deployment, use and ultimate disposal"*. Ann Cavoukian (Cavoukian, 2009) explained the 7 foundational principles on which principle by design is based:

- **Proactive not reactive** meaning that it aims to prevent any privacy invasive events prior to occurring rather than resolving with them after they have happened.

- **Privacy by default** suggesting that the maximum level of privacy should be automatically offered to the user by the system with no actions required on the part of the individual.
- **Privacy embedded into design and architecture** of IT systems and business practices not as an add-on but as an integral part to the system without diminishing its functionality.
- **Full functionality** meaning that trade-offs like privacy vs security are unnecessary and that both could be achieved.
- **Full lifecycle protection** concerning the entire lifecycle of data that is being protected from the moment it is collected and extends to retention and then deletion.
- **Visibility and transparency** to operations and component parts is provided to both users and providers therefore stated promises and objectives mentioned in privacy policies can be verified by all parties.
- **User centric** as bottom line, suggesting that the interest of the individual should come first for the operator by providing strong privacy defaults, appropriate notice and user friendly options.

Privacy by design also features on a Digital Agenda for Europe (European commission, 2010) where it is acknowledged that it would give data subjects more control over their data through data minimization, privacy by default and implementation of tools that limit unnecessary collection of data.

5.3 Oppositions and conflicting interests

The principle of privacy by design and the proposed regulations have been strongly opposed by providers of data processing services (Kuner, 2012) and social network providers such as Facebook who react against privacy by default by stating that it disregards the sharing of data which is the fundamental basis of social networks. This reflects the conflict of interests between the claims for privacy and the use of personal data as a moneymaking and transactional object. In particular, Facebook's approach towards the matter has been presented earlier and it's obvious throughout its privacy policy. Another

indication of the conflict of interests is the proposals made by the Committee on industry research and energy of the European parliament that aimed to restrict the range of applicability for this principle and in particular it states that privacy by default should take into account business models and global developments (Mitrou, Privacy by design).

Such interests are hard to ignore and serve as indicatives of intension and dimension of approaches that characterize the various legal aspects that arise over and over again. Adoption of privacy by design/default principle would result in revising privacy policies, services and application along with business models both of search engines and social networks.

Non technical approaches lack the power to enforce proposed changes to controllers. Policies and regulations are not mandatory and awareness needs to be raised. Laws dealing with personal information form an important tool but take too long to be developed and are generally used to solve matters after things go wrong whereas technical solutions attempt to prevent violations. Therefore the importance of the privacy by design principle is easily understood as it acts at the same time as a proactive feature, embedded into the system and offers the appropriate theoretical foundation underlying privacy.

6 Raising users awareness

Previously it was mentioned that users "*have few power over the actions that are performed followed their registration to the network*" and said that they are left with a choice. Truth is that more factors apply to this dilemma. Firstly, it is true that if users chose the road of solitude and absolute privacy both parties would be losing something. Facebook would be losing popularity and significant profits and users the opportunity to socialize and experience social networking at its full. Clearly that's the road that both parties would avoid walking.

The most walked path remains the other and much is known to where it leads in the end (mass media criticism, complaints on one hand and profit and indefinite data manipulation on the other). Both sides need to revision their perspective towards privacy. Users need to be informed of the dangers and how they can be protected from them and the network needs to be clear and not try to push users to their limits concerning over-sharing data.

In this section, ways of securing our data by using settings offered by Facebook and important things to keep in mind are presented.

6.1 Reading a privacy policy

Most of the people skip over the privacy policy when joining a SNS. However, users can gain a lot of useful information by reviewing the policy prior to joining the service. Any questions regarding the collection and usage of information will be answered there. Except for the information provided by the user the SNS may collect additional information in an ambiguous way through constant tracking of users' activities and actions outside the SNS

with the use of “cookies”. Always keep in mind that privacy policies can change and it’s highly unlikely those users will be informed and that these policies only cover the SNS and not any third party applications that interact with the website.

Due to the fact that policies are long and difficult to comprehend some key points to consider when reading them follow:

- **Start at the end**. The most important parts of a privacy policy are often at the end summarized and contact information for the company is provided for further questioning regarding the acquisition of personal information.
- **Canceling your account**. Look out for information concerning complete account deletion and what happens to the data afterwards. In most cases it’s difficult or confusing to cancel an account and information is kept by the SNS.
- **Duration that personal information is stored**. Some information may remain for a certain period (3 to 6 months), completely deleted (manually only) or kept in database for ever.
- **User complaints**. Look for physical/email addresses where users can make complaints. Some SNS work with independent companies to review their privacy practices and in that case users have to contact the independent company.
- **Who owns the data a user posts**. Does the user lose rights to data when he posts or he preserves them? Do the marketers need users’ consent to use their data for advertisements?
- **How will a SNS notify users about changes to the privacy policy**? Will changes be posted to the homepage or will it only be posted in the privacy policy itself? Can users connect with a public profile on the social network that will inform them of changes to the privacy policy, or is there a way to receive an email if changes are made?
- **Does the social network participate in seal programs**? Social networks that participate in third-party seal or certification programs show some level of awareness of privacy concerns. This also gives users another place to voice concerns if any should arise. Some well-known companies include the Better

Business Bureau, Verisign and Truste. However, never assume that a third-party certification means the social network will always respect users' privacy and security.

- Lastly try googling for other users' opinions on the matter or, for more thorough analysis, turn to tech related media.

Generally, policies put in paper the approach of the site towards privacy and data protection. New and existing users of SNSs should have an inside look to know what to expect or what they are dealing with. It would be wiser to know these things in advance and decide whether or not it coincides with the way users approach privacy as well. As a result, fewer unexpected leakage or unintended sharing would occur and therefore fewer complaints about loss of trust and deception by the network would make it to the media.

6.2 Recommended privacy settings for Facebook

Profile page contains most of the data a user decides to put in the system and share with the network. Most data is also acquired from this section of Facebook because privacy settings allow so as they are set to be accessible from everyone. There are a lot of people who consider privacy settings quite confusing so I will provide my proposals regarding the audience each piece of data, placed in a user's profile, should get.

Basic information

1. **Birthday** should be set *"show only day and month in my profile"* which takes out the year therefore hiding the age of the user and limiting the information that could be used to gain access to other personal information.
2. **Interested in**, **gender and languages** should you choose to provide them visibility should be set friends or only me.
3. **Religious, political views** should be set to friends or only me. Religion is extremely personal and should be set to only me. Based on this information you will be prompted to "like" pages with associated content.

Location information

1. **Current location** should be set to only me as there's no need for others to know such information.
2. **Hometown** should be set to friends only.

Contact information

Email address, mobile and other phones, full residential address with zip codes and street names although it isn't advisable to share them under any visibility option, the "only me" or in certain occasions "friends" settings could be helpful enough. Facebook provides all its members with a @facebook.com address and its visibility should be also configured.

Work and education

Education, work history and secondary school should be set to friends or custom if you want to connect with specific people from your workplace or university. Note that people will be able to search you based on information on education and university fields you provide.

Relationships and family

Relationship status, family members and lists of friends should be set to friends or only me for better privacy. Keep in mind that relationship and family listings link the profiles of the users taking part in the connection.

About you, favorite quotations and interests

1. **About me & favorite quotations** better be set to friends as there usually lays an amount of data describing the user and his personality
2. **Interests** including films, TV series, books and generally all pages you have liked should be set to "friends" so that general public can't get a screenshot of your personality.

History by year

This section seems to be the most privacy endangering of all. All activities concerning "**life events**" of the user are classified by year. I would strongly suggest that certain categories of this section should be left unfilled like

"loss of a loved one" or "*expecting a baby*" and *"overcame an illness"* as they pose a serious threat to privacy.

Profile picture and photos

1. **Profile picture.** Choose carefully a profile picture because it represents you and if it is offending or violates any of Facebook's criteria this could result in account suspension or removal of the photo. Preferable audience would be again friends.
2. **Photo albums.** The place where all photos are gathered. For better privacy set "friends" audience and avoid providing additional information like place date and time the photo was taken.

This concludes settings that resolve around data that is provided by the user. In contrast with Facebook's recommended settings a more private approach is being dictated. These settings just protect users and their data against other users of the network that could potentially exploit the misuse of default privacy settings and surely guarantee a higher level of privacy. Objections against disclosure of certain information are held like contact information, sexual orientation, religious/political beliefs and medical records. Last but not least always remember that full control over your data is lost the moment you decide to share it with your "friends".

6.3 General rules for social networking

As social networks are not only used for entertainment and information but also for disseminating our work and our profile it is very important to manage our privacy and to configure existing settings to our own benefit in order to avoid threats like the ones mentioned before. Some of the best practices are presented below:

- **Participate:** faced with the risks of leaving a trail that may harm your reputation, you could choose to publish absolutely nothing or only do so anonymously. This would be a great mistake as the worst would be leaving no trail at all, meaning not having any digital presence. In recent researches nearly 90% of recruiters admitted that they use social networks to research potential hires. Some of them also stated

that they use social networks as a screening process in order to choose between candidates. Not having a digital presence could be interpreted as a lack of transparency, a refusal to share information or even worse as someone with nothing to say and a technophobe or risk averse person.

- **Be respectful and appropriate:** while using SNSs you will eventually meet people from different cultures, religions and generally people with different opinions regarding e.g. politics or sports. It is important to respect any other different opinion and even when arguing be polite and calm.
- **Share but not over-share:** while using SNSs you are supposed to share content with other users. It is ok to comment on a photo or upload your favorite song but remember that not all information is meant to be shared. Some things should be kept private like information about your financial situation, home phone number or address, marital and family disputes, pictures of inappropriate situations such as being intoxicated and many others. - Some of these examples may seem like obvious things not to share on social networks but real life examples prove me wrong – Additionally status updates have reportedly facilitated robberies in many occasions, photos depicting the use of illegal substances led to legal action for its owner.
- **Consider carefully who you friend:** this does not apply only on the occasion that we don't know another user. One must be careful when adding as a "friend" people he supervises or his own supervisor and even if he connects with them he must place them in different groups so that he manages which of his actions will be visible to him. As seen earlier, friends' privacy settings may affect our data visibility and accessibility so it would be best to know all of our friends and to be able to agree over desirable privacy settings for the benefit of all parties.
- **Know the audience of your posts:** set the appropriate audience for each post (by manually selecting post by post or by creating groups of friends, coworkers, colleagues) to avoid getting caught red handed.
- **Use always HTTPS for safe browsing:** by default it is disabled

- **Use security and privacy settings:** privacy settings control how visible your information and pictures are on the site as well as on search engines and how they are shared. Every SNS site has plenty of security and privacy settings. Problem is that the default option in most (probably all) of them is public so you have to customize it to meet up your standards. It is important to note that these settings change from time to time without you being notified so you have to come back and check on them.
- **Use the appropriate tool:** there are plenty of websites offering the same services. You don't have to use them all but choose the ones that fit you the best. Review their privacy policy, how they use and who has access to your data and choose wisely.
- **Delete old accounts:** every time we open an account for an online service we are producing a small fragment of our digital presence. Some will stay with us and become a very important part of it, whereas others will be left behind, and perhaps even disappear. In other occasions, we will discover that a particular tool is not useful for us in that moment and situation, and so we will discard it, or perhaps leave it there, awaiting for that moment when it will become clear to us that it is time to add it to our toolbox. My suggestion is that when not using an account is best for us to delete it (even if it stays somewhere archived it may not be visible and searchable to other users) because there is a risk of someone else trying to digitally impersonate us and consequently be victims of identity theft or worse. Moreover some of these trails could be damaging for our work opportunities.
- **Do not spam, flame and cyber-bully/stalk-report inappropriate behavior:** regardless to say that if someone causes any of these threats he will face at best account suspension (spam/flame), defamation and even prison sentence (cyber-bullying). On the other hand if we experience any of these behaviors we should report to the responsible authority.
- **Finally remember that if it's on the web, even if it is set as private, it is published and archived somewhere.**

To sum up, these are some propositions we should keep in mind when joining or using SNS. Following these set of practices along with the ability to decide which information could jeopardize and harm our privacy, we could successfully use SNSs for our own benefit. A well informed user will not only help to maintain privacy but will also urge others to adapt the same approach on these issues. Aside from not using SNSs at all, end user education in collaboration with documented policies and more privacy enhancing settings, compose the most fundamental protection that exists.

7 Last thoughts and discussion

In this final chapter of the study, ways of enhancing data protection and users' privacy were presented. Modern ways dictate that internet and therefore social networks must be integrated into our daily lifestyle and all activities performed through the internet. As a result of this tendency, users should be better prepared and SNS better shield and enhance users' data and privacy.

Internet users have different educational backgrounds and not all of them are privacy or even technology geeks. Unless all people are informed of the consequences that reckless use of SNSs could have internet and SNSs won't be able to act on our aid and will favor those who try to exploit users' unawareness. More to that, awareness of users is a huge step towards privacy but won't suffice, there needs to be an actual collaboration to this side from SNSs as well.

Facebook's strategy so far has been all about exploitation of users and their data. Facebook isn't just another platform where users view data about others but it has transformed into a primarily profit-generation by advertising platform. Users are never asked if they want to receive advertisements or if they like their data to be harvested but they have to agree to these terms if they want to use Facebook. "*World will be better if you share more"* Facebook states but the real question is for whom? Sharing can also be interpreted by Facebook's behavior as selling information to advertisers. Facebook at its current state makes the world a better place for companies interested in advertising.

Nobody expects Facebook to stop using data to make profit because Facebook is a money-making company as well as a social network. However it can put some thinking into favoring more opt-in privacy policies which would allow users to give their actual consent to whether or not they want to be targeted by advertisements. What's also expected from Facebook is to start talking more and make his case for an era of openness more transparently.

Unless these issues are addressed, searches for "how to delete Facebook" on Google that have nearly doubled in volume over the past 2 years will increase. No revenues from advertisements can be generated when users don't put in their thoughts and preferences. Facebook will certainly look into that as fewer fan base mains less revenue from advertisements and since each member is worth 1.1 dollars to brands it's hard to neglect. Alternatives to this property-oriented concept that Facebook offers have already started to make their presence like Diaspora a non-commercial, non-profit internet platforms which defines itself as "privacy-aware, personally controlled, do-it-all, open source social network".

8 Conclusion

Subject matter of this study is to address privacy concerns of social networks that have gained significant publicity over the years. Within the context of this study social networks were discussed and the threats along with privacy issues that have been deriving from their use were addressed as an introduction. Facebook was examined as it is the leading social network and has consequently drawn much more attention than the rest social networks concerning privacy offered. An analysis over default privacy settings, constantly changing privacy policies and major threats affecting users' privacy was conducted in combination with Facebook's features and services. Then ways of securing users' data and enhancing privacy were proposed.

Facebook altered its perspective for privacy over the years adopting a more public approach concerning data sharing. This happened by constantly changing privacy settings and policies without informing in time users that were primarily affected. Users on their behalf, did not only have to worry about malicious users inside the social network but also for their privacy as they were left unprotected towards third parties (data brokers, advertisers, developers) and so trust between them was gradually lost.

For trust to be restored, steps towards privacy should be made by all involved. Users should be first educated and be informed of the dangers and the perils that the use of social networks can produce. They also need to be more careful when sharing sensitive and personal information. Facebook should firstly adopt more privacy oriented settings in addition to asking users consent over changes that affect the future of their data. Also the approach towards users and their data should be redesigned or reviewed by Facebook and its partners. A proposal was made stressing the importance of "*a) privacy-friendly default settings, which allow users to freely, specifically and explicitly consent to any access to their profile's content that is beyond their self-selected contacts and b) adequate*

information about purposes of data processing and warnings about privacy and security risks". (Working Party, 2009, article 29)

The bottom line of this study is that current privacy settings and policies favor disclosure over privacy and contradict or deliberately hide their purposes. These poorly designed settings exploit user unawareness and ignorance towards privacy risks. Still, everyone is free to make his own choices about revealing information according to his critical thinking, experience and judgment.

9 References

- DATA, M. O. S. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L, 281(23/11), 0031-0050.
- ENISA Position Paper No.1, Security issues and recommendations for online social networks, 2007
- Barnes, John (1954). "Class and Committees in a Norwegian Island Parish." *Human Relations*
- Barnes, Susan B. "A privacy paradox: Social networking in the United States."*First Monday* 11.9 (2006).
- Ellison, Nicole B. "Social network sites: Definition, history, and scholarship."*Journal of Computer-Mediated Communication* 13.1 (2007): 210-230.
- Acquisti, Alessandro, and Ralph Gross. "Imagined communities: Awareness, information sharing, and privacy on the Facebook." *Privacy enhancing technologies*. Springer Berlin Heidelberg, 2006.
- Dwyer, Catherine, Starr Roxanne Hiltz, and Katia Passerini. "Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace." *AMCIS*. 2007.

- Stutzman, Fred, Ralph Gross, and Alessandro Acquisti. "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook." *Journal of Privacy and Confidentiality* 4.2 (2013): 2.
- Grimmelmann, James. "Facebook and the social dynamics of privacy." *Iowa Law Review* 95.4 (2009): 1-52.
- Beye, Michael, et al. "Literature overview-privacy in online social networks." (2010).
- Information Gathering and Social Networks: Minimizing Exposure in the Digital Age, Erin Reid and Connie Pendleton, Davis Wright Tremaine, 2010
- Hargittai, Eszter. "Facebook privacy settings: Who cares?." *First Monday* 15.8 (2010).
- Schneier, Bruce. "Lessons from the Facebook Riots." *Wired, Sept* 21 (2006).
- Tuunainen, Virpi Kristiina, Olli Pitkänen, and Marjaani Hovi. "Users' Awareness of Privacy on Online Social Networking sites-Case Facebook." *22nd Bled eConference eEnablement: Facilitating an Open, Effective and Representative eSociety, Bled, Slovenia: http://ecom. fov. uni-mb. si/proceedings. nsf/0/9b675b5e811394f0c125760000390664/$ FILE/1_Tuunainen. pdf* (2009).
- Levin, Avner, and Patricia Sánchez Abril. "Two notions of privacy online." *Vand. J. Ent. & Tech. L.* 11 (2008): 1001.
- Tufekci, Zeynep. "Can you see me now? Audience and disclosure regulation in online social network sites." *Bulletin of Science, Technology & Society* 28.1 (2008): 20-36.
- Kosta, Eleni, et al. "Data protection issues pertaining to social networking under EU law." *Transforming Government: People, Process and Policy* 4.2 (2010): 193-201.
- Μήτρου, Privacy by Design Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων
- Papadopoulos, Marinos, and Alexandra Kaponi. "Privacy in the nook of Facebook."

- Turow, Joseph. *Americans & online privacy: The system is broken*. Annenberg Public Policy Center, University of Pennsylvania, 2003.
- Govani, Tabreez, and Harriet Pashley. "Student awareness of the privacy implications when using Facebook." *unpublished paper presented at the "Privacy Poster Fair" at the Carnegie Mellon University School of Library and Information Science* 9 (2005).
- Boyd, Danah, and Jeffrey Heer. "Profiles as conversation: Networked identity performance on Friendster." *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on*. Vol. 3. IEEE, 2006.
- Liu, Yabing, et al. "Analyzing Facebook privacy settings: User expectations vs. reality." *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. ACM, 2011.
- Cavoukian, Ann. "Privacy by design: The 7 foundational principles." *Office of the Information and Privacy Commissioner* (2011).
- Van Alsenoy, Brendan, et al. "Social networks and web 2.0: are users also bound by data protection regulations?." *Identity in the information society* 2.1 (2009): 65-79.
- Wong, Rebecca. "Social networking: Anybody is a data controller." *Available at SSRN 1271668* (2008).
- Kuner, Christopher. "Data protection law and international jurisdiction on the Internet (part 1)." *International Journal of Law and Information Technology* 18.2 (2010): 176-193.
- Kosta, Eleni, et al. "Search engines: gateway to a new "Panopticon"?." *Trust, Privacy and Security in Digital Business*. Springer Berlin Heidelberg, 2009. 11-21.
- Carminati, Barbara, Elena Ferrari, and Andrea Perego. "Security and privacy in social networks." *Encyclopedia of Information Science and Technology,* 7 (2009): 3369-3376.
- Leenes, Ronald. "Context is everything: sociality and privacy in Online Social Network Sites." (2010): 48-65.

- Jonathan Anderson, Claudia Daz, Joseph Bonneau, and Frank Stajano. Privacy-enabling social networking over untrusted networks
- Guha, Saikat, Kevin Tang, and Paul Francis. "NOYB: Privacy in online social networks." *Proceedings of the first workshop on Online social networks*. ACM, 2008.
- Tootoonchian, Amin, et al. "Lockr: better privacy for social networks."*Proceedings of the 5th international conference on Emerging networking experiments and technologies*. ACM, 2009.
- Buchegger, Sonja, and Anwitaman Datta. "A case for P2P infrastructure for social networks-opportunities & challenges." *Wireless On-Demand Network Systems and Services, 2009. WONS 2009. Sixth International Conference on*. IEEE, 2009.
- Shakimov, Amre, et al. "Privacy, cost, and availability tradeoffs in decentralized OSNs." *Proceedings of the 2nd ACM workshop on Online social networks*. ACM, 2009.
- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on Promoting Data Protection by Privacy Enhancing Technologies (PETs)
- Cotino, Lorenzo. "ARTICLE 29 DATA PROTECTION WORKING PARTY."
- Kuner, Christopher. "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law."*Bloomberg BNA Privacy and Security Law Report (2012) February* 6.2012 (2012): 1-15.