22nd Bled eConference

eEnablement:

Facilitating an Open, Effective and Representative eSociety

June 14 - 17, 2009; Bled, Slovenia

Users' Awareness of Privacy on Online Social Networking sites – Case Facebook

Virpi Kristiina Tuunainen [1]
Olli Pitkänen [2]
Marjaana Hovi [3]

1 Helsinki School of Economics, Finland
2 Helsinki Institute for Information Technology HIIT, Finland
3 Trainer's House Oyj, Finland

1 virpi.tuunainen@hse.fi
2 olli.pitkanen@hiit.fi
3 marjaana.hovi@trainershouse.fi

Abstract

Online social networking offers a new, easy and inexpensive way to maintain already existing relationships and present oneself to others. However, the increasing number of actions in online services also gives a rise to privacy concerns and risks. In an attempt to understand the factors, especially privacy awareness, that influence users to disclose or protect information in online environment, we view privacy behavior from the perspectives of privacy protection and information disclosing. In our empirical study, we present results from a survey of 210 users of Facebook. Our results indicate, that most of our respondents, who seem to be active users of Facebook, disclose a considerable amount of private information. Contrary to their own belief, they are not too well aware of the visibility of their information to people they do not necessarily know. Furthermore, Facebook's privacy policy and the terms of use were largely not known or understood by our respondents.

Keywords: Privacy, Social Networking Sites, Data Protection

1 Introduction

A social network is a set of people or other social entities such as organizations connected by a set of socially meaningful relationships (Wellman, 1997). Social networking sites (SNS) are a type of online communities that have grown tremendously in popularity over the past years. For example, the social networking site MySpace

(www.myspace.com) is ranked tenth in overall web traffic, with over 47 million unique US visitors each month (www.quantcast.com, 2008). Lately, especially the social networking service Facebook (www.facebook.com) has been receiving a lot of media attention all over the world, particularly because of privacy issues.

Facebook is now one of the biggest social networking sites. It was founded in 2004 in the USA by a former Harvard student Mark Zuckerberg. In the beginning, it was created only for students' use, but now it is open for everyone who has a valid email address. The success and growth of Facebook has been incredible: after the first year, it had already one million users, and five years later, in February 2009, Facebook had already more than 175 million active users. More than half of Facebook users are outside of college, and the fastest growing demographic is those 30 years old and older. Facebook had a powerful entry also to the Finnish market in the summer and early fall of 2007. In the spring of 2008, the Finnish Facebook network had over 399 000 users (www.facebook.com).

Members of a social network connect to others by sending a "Friend" message or request, which usually must be accepted by the receiving party in order to establish a link. By becoming "Friends", the members allow each other to access their profile information, and add each other to their corresponding social networks. However, users can always determine how visible their profile and profile information are. They can restrict the viewing of their profiles from people not part of their network, or they can keep the profile open for everyone.

In this study, we have mainly considered information disclosure in terms of profiles, i.e. what users reveal themselves in their profiles, but disclosing personal information may also occur in participation of discussions, writing messages in other users' pages, 'walls' and so on.

Earlier research (see e.g. Boyd & Ellison, 2007; Dwyer et al., 2007; Lehtinen, 2007) suggests that the main motivation to use online social networking sites is to communicate and to maintain relationships. Lehtinen (2007) found that different interaction rituals are performed on an SNS for reconstructing the established social networks. Popular activities include updating personal information and whereabouts ("status"), sharing photos and archiving events, getting updates on activities by friends, displaying a large social network, presenting an idealized persona, sending messages privately, and posting public testimonials (Dwyer et al., 2007).

Several studies have attempted to determine implications of privacy concerns and awareness of privacy to users' online practices and behavior (see e.g. Dinev & Hart, 2006; Dwyer et al., 2007; Goettke & Christiana, 2007; Govani & Pashley, 2005; Gross & Acquisti, 2005). The real privacy risks are believed to arise when users disclose identifiable information about themselves online to people who they do not know or normally (that is, offline, in real life) would not trust (see e.g. Brooks, 2007). This is assumed to stem from the users' lack of privacy concerns (Gross & Acquisti, 2005).

Govani and Pashley (2005) investigated student awareness of the privacy issues and the available privacy protection provided by Facebook. They found that the majority of the students are indeed aware of possible consequences of providing personally identifiable information to an entire university population (such as, risk of identity theft or stalking), but nevertheless, feel comfortable enough in providing their personal information. Even though they are aware of ways to limit the visibility of their personal information, they

did not take any initiative to protect the information (Govani & Pashley, 2005). In another study, Tow at al. (2008) conclude that users are often simply not aware of the issues or feel that the risk to them personally is very low, and have have a naïve sense that online communities are safe.

Social networking sites have a lot of users who have "an open profile" with considerable amount of personal information (e.g. photos, contact information, current "whereabouts status", and so on). Do these users feel comfortable with sharing all their personal information with a large number of strangers? Or do they actually know who can access their profile information? Are they concerned about their privacy?

In this study, we look at users' awareness of privacy on online social networking sites. Furthermore, we are interested in whether the awareness (or lack of it) influences users' privacy behavior.

We highlight two privacy perspectives: protection and disclosure. The two viewpoints are analyzed and we attempt to understand what influence users to disclose or protect information on Facebook.

This paper is organized as follows: We will next review earlier literature on online social networking, especially issues related to privacy and legal matters. We will then introduce our empirical study. After discussing the results of the study, conclusions are presented.

2 Online Social Networking and Privacy

Social networking sites (SNS) are online environments in which people create self-descriptive profiles and then make links with other people they know on the site (i.e., creating a network of personal connections). On many of the large SNSs, participants are not necessarily "networking" or looking to meet new people, but they are primarily communicating with people who are already a part of their extended social network (Boyd & Ellison, 2007).

Most SNSs provide a mechanism for users to leave public messages on their Friends' profiles. This feature typically involves leaving "comments," although sites employ various labels for this feature (Boyd & Ellison, 2007). In addition, SNSs often also have a private messaging feature, similar to webmail. SNSs can also offer discussion forums, groups or other communication features between users with same interests.

The public display of connections is a central component of social networking sites. After joining a social network site, users are prompted to identify others in the system with whom they have a relationship. The label for these relationships differs depending on the site, popular terms include "Friends," "Contacts," and "Fans." Most SNSs require bi-directional confirmation for Friendship, but some do not. The one-directional ties are sometimes labeled as "Fans" or "Followers," but many sites call these Friends, as well. The term "Friends" can be misleading, because the connection does not necessarily mean friendship in the same way it is used in everyday language, and the reasons people connect are varied (Boyd, 2004).

While SNSs have implemented a wide variety of technical features, their backbone consists of visible profiles that display an articulated list of Friends who are also users of the system. Profiles are unique pages where user can present her/himself as real or

"want to be". After joining an SNS, an individual is asked to fill out forms containing a series of questions. The profile is generated using the answers to these questions, which typically include descriptors such as age, location, interests, and an "about me" section. Most sites also encourage users to upload a profile photo. Some sites allow users to enhance their profiles by adding multimedia content or modifying their profile's look and feel. Others, such as Facebook, allow users to add modules, "applications," that enhance their profile.

The visibility of a profile varies by site and according to user discretion. By default, profiles on Friendster (www.friendster.com) and Tribe.net (www.tribe.net) are found by Internet search engines, making them visible to anyone, regardless of whether or not the viewer has an account. Alternatively, LinkedIn (www.linkedin.com) controls what a viewer may see, based on whether she or he has a paid account. Sites like MySpace allow users to choose whether they want their profile to be public or "for Friends only." (Dwyer et al., 2007) On Facebook, users who are part of the same "network", can by default view each other's profiles, unless the profile owner has decided to deny permission to those in their network.

2.1 Legal aspects of Privacy on SNSs

Today people communicate more and more using digital technology, such as e-mails, instant messengers, and social networking sites. When using different online services, for instance, e-shopping or the Internet forums, the users generate a wealth of data about themselves. These electronic footprints enable third parties to build up a picture of the users' behavior. Even if technology and information systems are a part of everyday life for most people in developed countries, modern information and communications systems are very complex and can be confusing: the users commonly have no idea what sort of data is being gathered about them, how much, where it is held, how long it will be held, and what it will be used for (German Federal and State Data Protection Commissioners, 1997).

From the legal viewpoint, privacy is mainly protected by general human and constitutional rights, and by more specific data protection rules. The European Union has been leading the development of the data protection law, which has arguably resulted sometimes even too strict rules. However, with respect to new kind of services, such as SNSs, the laws still fail to cover them adequately. The data protection law is designed to protect individuals against malicious criminals and overactive businesses, but it hardly stipulates social relationships between human beings.

In general, the European law restricts the processing of private data. For example, there has to be an acceptable purpose to process personal data and it is not allowed to use the data against that purpose. However, if the person gives consent, then almost any processing is allowed. In an SNS, people upload their private data into the service themselves. Therefore, arguably, the processing of that data is in accordance with their consent – as long as they have understood what kind of processing and usage of the data can take place. Thus, it is central what the end-user knows and understands about the privacy policy of an SNS and the principles according to which the data is processed. Just by publishing information, the end-user has probably not given consent to such processing that was unknown to him or her.(Kosta & Dumortier, 2008)

It should be noted that usually it is quite possible to develop all the services in a way that they comply with the data protection law. However, the legal construction of data

protection rules is quite complex. The rules governing privacy with respect to an SNS cannot be found in one law, but they are spread out in numerous statutes. Thus, it is also easy to develop services that do not follow the law, if the data protection law is neglected while designing the new service. (Pitkänen, 2006; Kosta & Dumortier, 2008)

It is important to realize that the data protection law is not prohibiting businesses and services, like an SNS, to avail of personal data. On the contrary, it tries to define a legal framework which enables business. Yet, new services, like SNSs, may find laws outdated.

2.2 Access to user's personal information

An important aspect on privacy risk is the question, who has an access to users' personal information shared on the internet and in the social networking site. Definition of personal identifiable information or personally identifying information (PII) is relevant when discussing online and internet privacy threats and risks. Personally identifiable information is any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. Understanding the concept of PII has become much more important as information technology and the Internet have made it easier to collect that information. (Kosta & Dumortier, 2008)

According to Gross and Acquisti (2005), three groups of stakeholders can access participants' personal information in an online social network: the hosting site, the network, and third parties.

The hosting site has access to participants' information, of course. The hosting site may use and extend the information in different ways. The information could be both knowingly and unknowingly revealed by the participant. (Gross & Acquisti, 2005)

The information is also available within the network itself. The network's extension in time (i.e. data durability) and in space (i.e. membership extension) may not be fully known or knowable by the participants. (Gross & Acquisti, 2005)

Third parties can access participants' information without the site's direct collaboration (Gross & Acquisti, 2005). The easiness to join and extend one's network, and the lack of basic security measures (such as cryptographic protocols for providing secure communications on the Internet, e.g. TLS/SSL logins) in most networking sites makes it easy also for malicious third parties, such as identity thieves, to access and misuse the users' information. In the case of Facebook, third parties with permission, that is, third party application providers, have a right to access users' data when a user adds their application.

When personal information is accessed by malicious third parties, additional risks associated with privacy become real. The nature of the risk depends on the type and the amount of information that has been provided: the information may, in certain cases, be extensive and very intimate. These online privacy risks range from identity theft to both online and physical stalking; and from embarrassment to price discrimination and blackmailing (Gross & Acquisti, 2005).

Unauthorized access to private information may cause economic losses to the individual. However, the SNS related privacy concerns are even more significant to both one's self-image and public identity. Loss of privacy and control over personal information may cause damages that are socially irreparable: losing face among friends, revealing secret information, making social blunders, or simply giving a wrong

impression. What makes these threats serious is that often the audience includes people with whom one has to interact everyday in the physical world. From the individual's perspective, therefore, these threats can have very serious consequences. For example, losing face among colleagues can be much worse than losing one's credit card number. These kinds of social problems have not, to our best knowledge, been studied earlier, and will remain an interesting avenue for future research.

2.3 Privacy policy of an SNS

As a response to the online privacy risks and threats, many website privacy policies specifically address the collection of personal information. Also the above mentioned data protection laws limit the distribution and accessibility of personal identifiable information. As discussed earlier, the privacy policy may clarify to which processing the user has given consent, when he or she has uploaded personal information into the service. Therefore, the relationship between the data protection law and the privacy policy is important.

A privacy policy is a notice on a website providing information about the use of user's personal identifying information by the website owner (particularly personal information collected via the website). Privacy policies usually contain details of what personal information is collected, how the personal information may be used, to whom the personal information may be disclosed, the security measures taken to protect the personal information, and whether the website uses cookies and/or web bugs (www.bbbonline.org, 2007). The exact contents of a privacy policy will depend upon the applicable law. For instance, there are significant differences between the European and the US data protection laws. At the moment, there are no well-known and generally used international privacy policy standards, yet. However, for example Google (www.google.com) has brought up discussion about international privacy standards which work to protect everyone's privacy on the Internet (www.googlepublicpolicy.blogspot.com).

Privacy features are technical implementation of privacy controls on websites. Privacy settings or tools are also generally used terms. A site should maintain standards of privacy and enable user friendly profile control and set-up to encourage safe participation.

Facebook and other SNS have been criticized for the fact that users' profiles are by default visible to an audience as wide as possible. If the users do not change their privacy settings, the information is available not only to their friends, but in the worst case also to everybody on same networking service. Gross and Acquisti (2005) have also present that the service provider's own user interface might be reason why people adjust settings so little. Anyhow, privacy features have no meaning, if the end-user does not use them. The study of Gross and Acquisti (2005) shows that only a small number of Facebook members change the default privacy references, which are set to maximize the visibility of the users' profiles. Cranor et al. (2006) noted that despite efforts to develop usable interfaces and features, most users rarely change the default settings on many of the software packages they use. The reason for why users do not change the settings can be the aspect of time consumption, confusion, or user's fear of risk to "messing up" their settings.

2.4 Privacy behavior of SNS users

Earlier research has shown that people have little knowledge about the real privacy risks in the online environment, and that they are unaware of the amount of personally identifiable information they have provided to an indefinite number of people (see e.g. Cranor et al., 2006; German Federal and State Data Protection Commissioners, 1997; Goettke & Christiana, 2007). Cross and Acquisti (2005) also suggest, that users may have relaxed attitude towards (or lack of interest in) personal privacy and myopic evaluation of the associated privacy risks.

For example, Facebook privacy policy tells that third parties can access and share certain personal information about the user (excluding contact information). Nevertheless, earlier studies have shown that users do not put effort to actually read the online social services' privacy policies and the terms of use (see e.g. Acquisti & Gross, 2006; Gross & Acquisti, 2005; Jones & Soltren, 2005). Cranor et al. (2006) noticed that users find learning about privacy and reading the website privacy policies to be difficult and time consuming.

Quite many users are aware of privacy features and know how to use them, but they do not take initiative to protect their information (see e.g. Acquisti & Gross, 2006; Dwyer, 2007; Govani & Pashley, 2005; Gross & Acquisti, 2005; Jones & Soltren, 2005). For example Acquisti and Gross (2006) show in their study that the majority of Facebook members claim to know about ways to control the visibility and searchability of their profiles, but only a significant minority (30% of students in their sample), are unaware of those tools and options. Jones and Soltren (2005) put the figures for students in their sample at 74% being familiar with the privacy feature, of which only 62% actually using the features to some degree.

Gross and Acquisti (2005) used Signaling Theory to analyze the types and amount of information disclosed on Facebook profiles. Signaling theory, which originates from evolutionary biology, has been lately been used to explain why a user shares personal information on SNSs. According to a number of studies (see e.g. Donath, 2007; Dwyer, 2007; Gross & Acquisti, 2005; Lampe et al., 2007), the users feel the need to present themselves and make a good impression on their peers. The study of Gross and Acquisti (2005) showed that the users (in this case students of Carnegie Mellon University) of Facebook provide astonishing amount of information, for example, their real name, photo(s), date of birth, phone number, current residence, and relationship status. "Users may be pragmatically publishing personal information because the benefits they expect from public disclosure surpass it perceived costs." (Gross & Acquisti, 2005, p. 80)

3 Empirical study

The target of the empirical part of the study is to collect data and analyze how much and to whom, Facebook users disclose information in their profiles and is there some certain influence factors. Also, the other objective is collect data of users' attitudes and awareness of Facebook privacy and explore do they affect users information disclosing.

3.1 Research methodology

The empirical data was gathered with a web questionnaire. This method was natural choice because of research subject (users' behavior on the Internet). The first aim of the questionnaire was to find out background information of respondents and then collect

the actual data about users' information disclosing in profiles, users' privacy and security concerns and finally their awareness of privacy on Facebook. Variables were measured with categorical, scale, and non-metric variables. Also some open questions were used for feedback questions. The questionnaire consisted of five main parts: 1) background information; 2) User's personals information and friends on Facebook; 3) User's privacy controlling / setting; 4) User's privacy and security concerns; and, 5) User's awareness of Facebook Privacy Policy (and open feedback question). For the lack of available space, the full questionnaire is omitted from this paper, but can be acquired from the authors.

160 Facebook users were invited to answer this questionnaire via Facebook. Invitation receivers had the possibility to invite more users to answer the questionnaire. The questionnaire was available for eleven days. As a second method, a convenience sample was used to ask people to answer the questionnaire via e-mail. E-mail was sent to 20 people. All of these people were Facebook users, but normally log in Facebook very rarely. These users had also the possibility to send the invitation forward. Using the snowball effect a total number 210 acceptable responses were received.

3.2 The Social Networking Site under study: Facebook

Facebook was established in February 2004 and by the end of the same year it already had one million users. At the time of our survey in April 2007, Facebook had over seventy million active users all over the world. Facebook had a powerful entry to the Finnish markets in the summer and early fall of 2007, and by Spring of 2008, the Finnish Facebook network had over 399 000 users. Probably there are much more Finnish users, because all Finnish users do not join to Finland-network (or any other network). Our empirical study, in which this paper is based on, focused on this Finnish Facebook user group.

A Facebook profile is like one's own page and the user can manage its information. Normally users create a Facebook profile with real name and profile picture, because nature of SNS. In addition, users can share a multitude of different types of data with other users. These types of data include for example contact information, personal information like gender, birth date, hometown, education and work information, information regarding interest movies, music, clubs, books, relationship status and partner's name, and political orientation. Users can in fact choose to fill in any of this information fields and update their information at any time. Users can also share photos and videos with other users.

Users can communicate with others by using "profiles' 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 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.

Facebook has a various scales of privacy features. Users can control their profiles' visibility and also separate information fields in their profiles. Visibility options (who can see one's profile or other information) are normally "no one", "only my friends", "some of my networks and all my friends", and "all my networks and all my friends".

4 Findings

We will first introduce the sample and the background information of the respondents in general. Then users' information disclosing in profiles is presented. Afterwards, the privacy concerns and the awareness of privacy protection are discussed. Finally, some findings on privacy behavior are discussed.

Total number of 210 people responded to the questionnaire. Of these 56 % were females, 43 % males, and 1 % did not disclose their gender. 88% of the respondents were under 30 years old but over 18 years. Most of the respondents (74%) were students and only 26 % non students; The large number of HSE (Helsinki School of Economics in Helsinki, Finland) students (more than half of respondents) stems from the fact that the request was sent primarily to the friend list of the primary researcher, and more than half of them were HSE students.

Facebook is a fairly new phenomenon, also in Finland, and therefore it is natural that most of the responders (67%) had had a profile less than half year. Almost everybody (92 %) had stated their reason to join Facebook as "friend suggested it". The second common reason was to "make easier to keep in touch" (60 % had check this option). "Find classmates", "Everyone I know is on Facebook", and "to network in general" were also common reasons to join Facebook. These results show that networking in general and communication are main causes to create a profile and in effect to disclose information.

The respondents' number of friends varies a lot: 17 % have 50 or less, while 9 % have more than 350 friends. Mostly the respondents have invited their "close friends" (92%) or "friends" (96%) to become Facebook Friends with them, enforcing existing strong connections. However, well more than half (65%) of the respondents have also invited "people they just know" to their Friends, as well as "people they have just met once (12%) and "people whom you haven't met" (3%). Similar figures are true for accepting invitations from others.

All of the respondents log into Facebook at least once a week, 86 % once or more than once a day. 55 % of all respondents update their "status" (once a week or more than once a week, while 23 % of respondents never update their status on Facebook.

4.1 Information disclosing

The respondents share a large number of information about themselves on Facebook. Only two respondents of 210 informed that they did not appear with their real names on Facebook. More than 90 % of respondents had a profile picture on their profiles. More than 80 % had information like one's hometown, the date of birth, e-mail address and education info. 75 % of respondents had pictures of them and more than 60% had pictures of their friends. Almost 60 % of respondents presented their relationship status on the profile. (See table 1. for a summary of the information provided by the respondents.) With the maximum of 17 different items, the respondents had, on average, checked 9.4 items.

Table 1: Personal information on profile

Questionnaire item	n	%
Real name	208	99
Profile picture	206	98
Birthday	186	89
Home town	186	89
E-mail address	174	83
Education information	169	80
Photos of one's self	158	75
Photos of one's friends	130	62
Relationship status	124	59
Sexual orientation ("interested in")	103	49
Favorite music, movies, etc.	70	33
Contact phone number	69	33
Activities / interests	67	32
Partner's name	55	26
Street address	38	18
Website	25	12
Political views	20	10

Presented in the order of frequency

Furthermore, the general rule seems to be that, the more details is provided in the profile, the more active user of Facebook the respondent is: a greater number of Friends, more groups joined, and more active status updating behavior.

When examining users information disclosing the question is not only "how much information is disclosed", but also "whom the information is disclose to". Users of Facebook can limit the visibility of the profile by choosing between the three options "my friends and my networks (or some of networks)", "only my friends", or "only me / no one". The majority of respondents have allowed access only for their friends (63%). Still, there are many (34%) who keep their profiles open to all the users part of the same network. There does not seem to be a great difference between the number of different items displayed on the profile between those whose profile is open and those whose profile is visible to Friends only.

4.2 Privacy protection

It seems that the respondents are slightly worried about their privacy when using the Internet. Also using credit card within the Internet seems to bring concerns. The respondents do not seem to have many concerns about other people on the Internet, but they rather seem to trust the other users on the Internet. They still think that an identity

theft could be a real privacy risk. The respondents are also pretty familiar with data protection and security while using the Internet in general (see Table 2.).

Table 2: Privacy and data security concerns in general

Questionnaire item	Avg.	Mode	SD	n
I worry about my privacy and data security while using the internet	4,5	5,0	1,6	209
I worry that if I use my credit card to buy something on the internet my credit card number will be obtained / intercepted by someone else	4,3	5,0	1,7	210
I worry about people online not being who they say they are	3,7	2,0	1,5	210
I feel that identity theft could be real privacy risk	4,5	5,0	1,6	210
I worry that if I use internet with my mobile phone and someone steals it, he/she can find out some of my personal information or data	3,2	2,0	1,8	210
I'm familiar with data protection and securing while using the Internet in general	4,8	5,0	1,6	210

Measured on 1-7 scale (1 = strongly disagree, 7= strongly agree)

Results of privacy concerns on Facebook reveal that the respondents do not have notable concerns about privacy and data security while using Facebook (see Table 3.).

Table 3: Privacy and data security concerns on Facebook

Questionnaire item	Avg.	Mode	SD	n
I worry about my privacy and data security while using Facebook	4,0	2,0	1,7	210
I feel that the privacy of my personal information is protected by Facebook	3,9	5,0	1,5	210
I trust that Facebook will not use my personal information for any other purpose	4,3	6,0	1,6	210
I feel comfortable writing messages on my friends' walls	5,2	6,0	1,4	210
I worry that I will be embarrassed by wrong information others post about me on Facebook	3,5	2,0	1,7	209

Measured on 1-7 scale (1 = strongly disagree, 7= strongly agree)

Compared to responses about privacy concerns in general, the respondents seem to be more worried about privacy when using the Internet in general, than when using

Facebook in particular. Also, it seems that, by and large, the respondents trust Facebook with their private information.

Majority of the users (75%) say that they know who can see their profile in it, while 29 % either do not know or are not sure (see Table 4.)

Table 4: Visibility of profile information

Questionnaire item	Yes	%	No	%	Not sure	%
Do you know who can see your profile and the information in it?	158	75	8	8	44	21

Response: Yes/No/I am not sure (total n=210)

Almost all of the respondents (94 %) are aware that the privacy settings can be modified, and the majority (84 %) say that they have done so (see Table 5). Also, the respondents claim to be knowledgeable about the fact that without modifying their privacy settings, their profile will be visible to the members of all new networks they join.

Table 5: Privacy settings

Questionnaire item	Yes	%	No	%	n
Are you aware that you can change your privacy settings?	197	94	12	6	209
Have you ever used your privacy setting?	164	84	32	16	196
Are you aware that if you have joined some network and you haven't changed your privacy setting, all members of same network can see your profile?	160	76	50	24	210

Response: Yes/No

The possibility for third parties to access users' profile information is not as well acknowledged (see Table 6): over half (55 %) of the respondents did not know that if a user adds an application, the developer of the application has a right to access the user's information. Furthermore, the majority (73 %) is not aware, that Facebook can, according to their privacy policy share the users' information with outside parties for marketing purposes.

Table 6: Sharing information with third parties

Questionnaire item	Yes	%	No	%	n
Are you aware that when you add a new application (e.g. Entourage/Fun wall), you give the organization that supplies the application, the right to access your profile information?	93	45	115	55	208
Are you aware that Facebook can share your information with people or organisations outside of Facebook for marketing purpose as their privacy policy?	57	27	153	73	210

Response: Yes/No

Then again, only 21 % of the respondents have read the Facebook privacy policy, and even fewer (15 %) have read the Facebook terms of use (see Table 7).

Table 7: Privacy settings

Questionnaire item	Yes	%	No	%	n
Have you read the Facebook terms of use?	31	15	179	85	210
Have you read the Facebook privacy policy?	57	21	153	79	210

Response: Yes/No

Interestingly enough, over half (61%) of those who say they have read the Facebook privacy policy, are not aware of Facebook's right to share their information with third parties.

At the end of the questionnaire the respondents were asked if they thought that participating in the survey would affect their behavior on Facebook in any way. About two thirds (62%) thought it will. Of these 130 respondents, 109 took the time to answer to the "If yes, how?" question. Most comments are along the lines of "being more careful in the future" and "certainly now adjusting my privacy settings". As many as 31 mention specifically the Facebook add-on applications, and admit not having realized the information access they have provided to third parties. This indicates that increasing awareness of privacy might and will affect the user behavior: clear and compact information about privacy issues, features and practices makes users think about privacy and might result in more careful behavior in online environment.

5 Discussion

Online social networking offer new opportunities for interaction and communication. The online environment is an easy and inexpensive way to maintain already existing relationships and present oneself to others. However, the increasing number of actions in online services also gives a rise to privacy concerns and risks.

Our study shows, that the users of Facebook seem to disclose a large amount of information on themselves to a large amount of both strong and weak connections, sometimes to people totally strangers to them. As in most similar studies, our subjects are mostly young adults and students. The results show that they do not have significant privacy concerns, but claim to be fairly aware of privacy risks. Overall, the privacy risks are perceived to be smaller on Facebook than on the Internet in general. One reason for this can be the fact that "the Internet" is something vast and vague, while Facebook is perceived to be a more manageable "network of friends". It is very likely, that a great number of people, who do not use social networking services, do so exactly because of privacy concerns. However, as our sample only included (active) users of Facebook, that question remains to be looked at in future research.

As discussed above, privacy policies seem to be important. That is not only because they inform the users about the processing of private data, but also because they partly define consent that the users have given, when they have uploaded their private data into the service. Therefore, an interesting question for future research is why the users do not read privacy policies of SNS's. Like also other studies (e.g. Acquisti & Gross, 2006; Gross & Acquisti, 2005; Jones & Soltren, 2005) have shown, privacy policies and the terms of use just do not get the attention of the users. There might be several reasons for this: it is perceived to take too much effort, they are difficult to understand, or the users trust the service provider so much that they feel they do not have to read policies. Nevertheless, as our study shows, even reading the privacy policy does not seem to increase awareness of service provider practices.

Most of the users are – or claim to be – aware of privacy features on SNSs and they have also used them. However, default settings can seem confusing and some particular actions, for instance, joining a new network, might change settings without users realizing it. Furthermore, there are still many users whose profiles are highly visible to all the members of a particular network, which might include hundreds of thousands of strangers. Therefore, it remains an interesting question to which processing of private data the user has knowingly given his or her consent.

6 Summary and Conclusions

In this paper, we have reviewed earlier research on privacy issues related to social networking sites, and presented the results of our empirical study among users of a particular SNS, Facebook.

We have viewed privacy behavior from two perspectives: privacy protection and information disclosing. Both of these aspects were analyzed and used in attempt to understand the factors, especially privacy awareness, that influence users to disclose or protect information on Facebook.

In our empirical study, we surveyed users of Facebook, and acquired 210 usable responses. Our results indicate, that most of respondents, who seem to be active users of Facebook, do disclose a considerable amount of private information of themselves, and contrary to their own belief, are not too well aware of the visibility of their information to people they do not necessarily know. Furthermore, the privacy policy and terms of use of Facebook were largely not known or understood by our respondents. This was particularly true as regard to Facebook's policy of allowing third party application

providers access to the users' information. Encouragingly, however, many of the respondents were awakened by the survey, and resolved to pay more attention to their privacy settings in the future.

As the whole online environment and social networks in particular are fairly new phenomena, number of issues are not fully understood by the users, who might even appear to behave irrationally. Privacy is a complex construct and, as such, difficult to understand. Accordingly, there are many different factors that affect privacy behavior. Hence, more research into privacy awareness and related behavior on social networking sites is clearly called for.

In the next step of our study, we will perform a deeper analysis of our empirical data to better understand how the users interpret the construct of privacy, both conceptually and in practice.

References

Acquisti, A. and Gross, R., Imagined communities: awareness, information sharing, and privacy on the Facebook. From PET 2006. (Cambridge, June 28--30, 2006,

Boyd D., "Friendster and publicly articulated social networking", in the Proceeding of Conference on Human Factors and Computing Systems (CHI 2004), Vienna, Austria, April 24-29, 2004.

Boyd, D., and Ellison, N., "Social network sites: Definition, history, and scholarship", Journal of Computer-Mediated Communication, 13(1), 2007.

Brooks, G. 2007. "Secret society", New Media Age, 13 December, p. 10.

Clark, H.H. Using Language, Cambridge University Press, Cambridge, UK, 1996.

Cranor L., Gudruru P. and Arjula M., "User Interfaces for Privacy Agents", ACM Transactions on Computer-Human Interaction, Vol. 13, No. 2, June 2006, pp. 135–178.

Dinev, T. & Hart, P. 2006. "Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact", International Journal of Electronic Commerce, Vol. 10, No. 2, pp 7-29.

Donath, J., "Signals in social supernets", Journal of Computer-Mediated Communication, 13(1), 2007.

Dwyer, C., "Digital Relationships in the 'MySpace' Generation: Results From a Qualitative Study", in the Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS), Hawaii, 2007.

Dwyer C., Hiltz R., and Passerini K., "Trust and Privacy concern within social networking sites: A comparison of Facebook and MySpace", in the Proceedings of AMCIS 2007, Keystone, CO, 2007.

German Federal and State Data Protection Commissioners, Privacy-enhancing technologies, Working Group on "privacy enhancing technologies" of the Committee on "Technical and organisational aspects of data protection" of the German Federal and State Data Protection Commissioners, 1997.

Goettke R. and Christiana J., "Privacy and Online Social Networking Websites", http://www.eecs.harvard.edu/cs199r/fp/RichJoe.pdf, 5 Nov, 2007)

Govani, T., and Pashley, H.," Student Awareness of the Privacy Implications while Using Facebook" Unpublished manuscript retrieved 1 Nov 2007 from http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf, 2005

Gross, R. and Acquisti, "Information Revelation and Privacy in Online Social Networks (The Facebook case)", in the Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 2005, pp. 71 – 80.

Jones, H., and Soltren, J.H., Facebook: Threats to Privacy, MIT, Dec. 2005.

Kosta, E. and Dumortier, J.," Searching the man behind the tag: privacy implications of RFID technology", International Journal of Intellectual Property Management (IJIPM), Special Issue on: "Identity, Privacy and New Technologies", 2008.

Lampe C., Ellison N., and Steinfield C., A, "Familiar Face(book): Profile Elements a Signals in an Online Social Network", in the Proceedings of the SIGCHI conference on Human factors in computing systems CHI '07, March 2007, pp. 435 – 444.

Lehtinen, V., Maintaining and Extending Social Networks in IRCgalleria, University of Helsinki, Faculty of Social Sciences, Department of Social Psychology, Master's Thesis, May 2007.

Newk-Fon Hey Tow, W., Dell, P., Venable, J.R. (2008), "Understanding Information Disclosure Behaviour in Australian Facebook Users", the 19th Australasian Conference on Information Systems (ACIS) 2008, Christchurch, New Zealand, December 3-5, 2008.

Pitkänen, O., "Technology-Based Research Agenda on the Data Protection Law", in the Proceedings of LawTech 2006, Cambridge, MA, USA, 2006.

Wellman, B., "An Electronic Group Is Virtually A Social Network". In Kiesler, S., Culture of the Internet, New Jersey: Lawrence Erlbaum Associates, 1997, pp. 179-209.