Disclosing Personal Data Socially – an Empirical Study on Facebook Users' Privacy Awareness

Olli Pitkänen, Aalto University, Helsinki Institute for Information Technology HIIT, Finland, olli.pitkanen@hiit.fi

Virpi Kristiina Tuunainen, Aalto University School of Economics, Dept. of Information and Service Economy, Finland, virpi.tuunainen@aalto.fi

ABSTRACT

Maintaining existing relationships and present oneself to others is easy and inexpensive in social network services, such as Facebook. Nevertheless, the ever-increasing amount of personal data in these online services gives a rise to privacy concerns and risks. In an attempt to understand the factors, especially privacy awareness, that influence users to disclose or hide information in online environment, we view privacy behavior from the perspectives of privacy protection and information disclosing.

Our survey of 210 Facebook users indicates, that most active users of this social network service disclose a considerable amount of private information. Contrary to their own beliefs, 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 are largely either not known or understood. With the proliferation of different social media tools and services and the increased interest and involvement of companies and other organizations, understanding users' privacy attitudes and behavior becomes of paramount importance.

KEY WORDS

Privacy, Social Network Services, Data Protection

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 network services (SNS) are a type of online communities that have grown tremendously in popularity over the past years. Boyd and Ellison (2008, p.211) define social network sites as "*web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others*

within the system". Alexa.com, a web based service providing Internet usage statistics, informs that in March 2012 the leading SNS Facebook (http://www.facebook.com) was the number two in the list of most popular sites on the Web, second only to web searching giant Google. YouTube (social video-sharing website, http://www.youtube.com/) was the number three. (http://www.alexa.com/topsites, accessed: March 31, 2012)

A former Harvard student Mark Zuckerberg founded Facebook in 2004 in the USA. In the beginning, it was meant only for students' use, but it was soon opened 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 now, in March 2012, it has 845 million active users (http://ansonalex.com/infographics/facebook-user-statistics-2012-infographic/ accessed: March 31, 2012), approximately 80% of them outside the U.S. and Canada, and about half of them are using Facebook mobile products. Facebook is available in more than 70 languages, including Finnish.

Members of a social network connect to others by sending a "*Friend request*," which usually needs to be accepted by the receiving party in order to establish a link. By becoming "*Friends*", the members allow each other access to their profile information, and add each other to their corresponding social networks. However, with privacy settings of the social network service, users can always determine how visible their profile and profile information are: they can restrict the visibility of their profiles to the people part of their network, or they can keep the profile public, that is, open to everyone.

In this study, our main focus is on information disclosure in the context of SNS profiles, more specifically, on what the users reveal about themselves in their profiles. Disclosing personal information may also occur in updating the user's own "*status*", commenting of participation in discussions, writing messages in other users' pages, or "*walls*", and so on.

Earlier research (see e.g. Boyd & Ellison, 2008; Dwyer et al., 2007; Ross et al., 2009) suggests that the main motivation to use online social network services is to communicate and to maintain relationships. When considering individual functions available in a given SNS, varying motivations have been suggested to be influential in the user's decision to use these tools (Ross et al., 2009). Commonly available and popular functions 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.

Lampinen et al., 2011; Boyd & Hargittai, 2010; Lehmuskallio, 2009; Lampinen et al., 2009; Dinev & Hart, 2006; Dwyer et al., 2007; Goettke & Christiana, 2007; Gross & Acquisti, 2006; Govani & Pashley, 2005). Privacy risks arise when users disclose identifiable information about themselves online to people who they do not know or whom they would not trust offline, in real life (see e.g. Brooks, 2007). This kind of behavior is assumed to stem from the users' lack of privacy concerns (Gross & Acquisti, 2006).

Govani and Pashley (2005) investigated students' 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 the 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 privacy issues or feel that the risk to them personally is very low, and have a naïve confidence in safety of online communities.

Lampinen et al. (2011) have shown that users' management of privacy and public-ness in SNSs is largely based on expectations of others' attentiveness to one's self-presentation, both in how they behave and in the interpretations they make. Boundary regulation, meaning the balance between making some content public and keeping other things more private, relies largely on unspoken expectations of reciprocal attentiveness. However, reliance on unspoken expectations makes SNS users sensitive to unintended harm caused, for example, by a friend uploading indiscreet photos or making hasty comments. Despite the common good will of not wishing to cause trouble for others, blunders happen and actions can have unexpected outcomes.

Different social network services, Facebook included, have a great number of users who have a publically available, open profile, with considerable amount of personal information (e.g. photos, contact information, current location information, and so on). Do these users feel comfortable with sharing all their personal information with a large number of people they do not know? Or do they actually know who can access their profile information? Are they concerned at all about their privacy?

In this study, we look at users' awareness of privacy on online social network services. Furthermore, we are interested in whether the awareness (or lack of it) influences users' privacy behavior. We highlight two behaviors related to privacy: protection and disclosure. These two processes are analyzed with an

attempt to understand what influences users to disclose or protect information on Facebook.

This paper is organized as follows: In the next section we will review earlier literature on online social network, especially issues related to privacy and legal matters. We will then introduce our empirical study. After discussing the results of the study, conclusions and directions for future research are presented. Our survey instrument is also provided at the end of this study for your reference. Throughout the paper several tables with our key results are presented to support our assertions.

ONLINE SOCIAL NETWORKING AND PRIVACY

Social network services (SNS) are online environments in which people create self-descriptive profiles and then make links with other people they know on the service (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, 2008).

Most SNSs provide a mechanism for users to leave public messages on their Friends' profiles. This feature typically involves leaving "*comments*," although services employ various labels for this feature (Boyd & Ellison, 2008). 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 links or connections is a central component of social network services. After joining a social network service, users are prompted by the system to identify others with whom they have a relationship. The label for these relationships differs depending on the service, popular terms include "*Friends*," "*Contacts*," and "*Fans*." Most SNSs require bi-directional confirmation for the link or connection, but not all do. The one-directional ties are sometimes labeled as "*Fans*" or "*Followers*," but many services call these Friends, as well. The term Friend can be misleading, because the link does not necessarily mean friendship in the same way it is used in everyday language, and the reasons people connect vary (Boyd, 2004), depending on, for instance, whether the two person connecting know each other from work or from private life.

While all 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 - with facts or fiction. 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 services also encourage users to upload a profile photo. Some services allow users to enhance their profiles by adding multimedia content or modifying their profile's look and feel in different ways.

The visibility of a profile varies by service and according to user discretion. By default, profiles on for example tribe.net (http://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. Services like MySpace (http://www.myspace.com/) allow users to choose whether they want their profile to be public or "*for Friends only*." (Dwyer et al., 2007) On Facebook, users may choose whether their profile information, status updates, comments, and other information are public or visible only to their friends, or they may modify the visibility in more detail.

Legal Aspects of Privacy on SNSs

Today people communicate more and more using digital technology, such as e-mails, instant messengers, and social network services. When using different online services, for instance, e-shopping, blogs, 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 broad and too strict rules. For example, all the ordinary electronic address books in mobile phones or computers, which are not for a purely personal or household activity, but for also work or other non-private purposes, are subject to the data protection law (see the data protection directive 95/46/EC, Art 3). Thus everybody should notify the supervisory authority about the work-related phone books or, in accordance with national laws, at least make available a person file description in an appropriate form to any person on request (Art 21). It is obvious that we all have such electronic address or phone books and none of us has ever notified

the supervisory authority of them or created a person file description on them. The law, from this point of view, is absurdly broad. However, with respect to new kind of services, such as SNSs, the law does not cover them completely. The data protection law is designed to protect individuals against malicious criminals and overactive businesses, but in SNS the problems often arise from other sources: losing face among friends and colleagues can be worse than receiving unsolicited marketing messages or even being a victim of a criminal act. The law hardly stipulates social relationships between human beings, and for good reason: the lawmakers should be very moderate in regulating private relationships. Therefore, the most severe privacy problems in SNS are hardly legal, but should be controlled by social norms. (Pitkänen, 2006; Lampinen et al., 2011)

In general, the European law restricts the processing of private data. For example, there has to be an acceptable purpose, such as, customer relationship or membership, 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) For example, if the service provider adds a new functionality to the service and enables new ways to avail of personal data, the user's prior consent does not cover this new processing of old data.

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, if the data protection law is overlooked, designers can easily end up producing new services that do not comply with the law. (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, and as mentioned above, the law does not stipulate some of the most important privacy issues.

Access to User's Personal Information

An important question related to privacy risks is who has an access to users' personal information shared on the Internet and in the social network services. 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 that can potentially be used to uniquely identify, contact, or locate a single person. Understanding the concept of PII has increased in importance as information technology and the Internet have made it easier to collect that information. (Kosta & Dumortier, 2008)

SNS participants reveal information about themselves both deliberately and unintentionally (Gross & Acquisti, 2005). Gross and Acquisti (2005) identified three different groups of stakeholders that can have (or be given) an access to the participants' personal information in an online social network: the hosting service, the network, and third parties. The hosting service has, of course, access to the participants' information. The service may use and extend the information in different ways. For example, while the user is logged into the service, information can be gathered on the usage and use behavior, and the service experience can then be customized based on that information.

The users' 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 comprehensible by the participants. (Gross & Acquisti, 2005)

Third parties can access participants' information without the service's direct collaboration (Gross & Acquisti, 2005). The ease of joining and extending one's network, and the lack of basic security measures (such as cryptographic protocols for providing secure communications on the Internet, e.g. mandatory TLS/SSL logins) in most social networking services make it easy also for malicious third parties, such as identity thieves, to access and exploit 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.

By disclosing personal information to friends, the user exposes oneself to embarrassing situations, but when malicious third parties, additional risks associated with privacy become real, accesses the information. 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 even lead to economic losses for the individual. However, the SNS related privacy concerns are even more significant to both one's public identity and self-image. 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 perceived much worse than losing one's credit card number.

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, a privacy policy may clarify the kind of processing the user has given consent to, after he or she has uploaded personal information into the service. Therefore, the relationship between the data protection laws and the privacy policies is important.

The privacy policy of a service is presented on the service's website, and it provides 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 technologies like cookies or web bugs to track information on web browsing habits. 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.

Different privacy laws may apply to the same SNS if a user is accessing the service, say, from the USA, Europe, or Asia. That may put the service provider in a quite difficult situation and lessen legal foreseeability. For example, it is hard to find out, which information should be provided for the users according to each national or state law, and what legal consequences there might be, if the service provider fails to provide all the necessary information. Furthermore, it can be difficult for the user to find out, which rules are applicable. As of 2012, there are no privacy policy standards with international coverage. However, for example the Electronic Frontier Foundation (EFF) has brought up discussion about international privacy standards, which work to

protect everyone's privacy on the Internet (https://www.eff.org/issues/international-privacy-standards).

Privacy settings or tools, also called as privacy features, are technical implementation of privacy controls on websites. A service should enable user-friendly profile set-up and control to encourage safe participation and practices.

Facebook and other SNS have often been criticized for the fact that users' profiles are by default visible to an audience as wide as possible. If the users do not modify their privacy settings, the information is available not only to their friends, but in the worst case, to everybody using the same networking service. It has been suggested that the typical user interface of a SNS does not readily encourage changes to the privacy settings, and that this might be driving the unchallenged acceptance of permeable default settings (Gross & Acquisti, 2005). In any case, privacy features have no meaning, if the end-users do not use them. It has been 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 (Gross & Acquisti, 2005). 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.

Privacy Behavior of SNS Users

Earlier research has shown that people have little knowledge about the various 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 states that third parties may access and share certain personal information about the user. 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). Furthermore, users have been found to perceive learning about privacy and reading the website privacy policies to be difficult and time consuming (Cranor et al., 2006).

Quite a few 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; Debatin et al., 2009; 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 users 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.

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. Gross and Acquisti (2005) showed that the users of Facebook (university students in this case) provide surprising 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)

EMPIRICAL STUDY

The aim of our empirical study was to understand the users' privacy behavior on social network services. To this end, we collected data and analyzed how much and to whom, Finnish Facebook users disclose information in their profiles and whether there are any particular factors influencing their behavior. Furthermore, we were interested in the users' attitudes and awareness of Facebook's privacy policy and practices, and on what kind of effect they had on users information disclosing.

Case Context: 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 even already then, there were much more Finnish users, because not all of them had joined the "*Finland network*", in other words, they had not indicated their Finnish nationality. Our empirical study 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 of the nature of SNS. In addition, users can share a multitude of different types of information with other users. These can include,

for example, contact information; personal information such as gender, birth date, hometown, education and work information; information regarding interests related to movies, music, clubs or books; relationship status and partner's name; and political orientation. Users can choose to fill in any, all or none of this information and update or modify it at any time. Users can also share photos and videos with other users.

Users can communicate with others by using "*profiles*", "*walls*" or private messaging features. A writing on other user's wall is normally visible to everybody who has access to this profile and information in it. Users also can comment on each other's photos, videos or other posted elements. With using "*status updates*" users can also communicate to other people in their network what they are doing or thinking about, and so on, and with location information where they are.

Facebook offers a range of different privacy features. Users can control their profiles' visibility and also separate information fields in their profiles. Visibility options, meaning who can see one's profile or other information, are normally "*no one*", "*only my friends*", and "*everybody*", but recently Facebook has introduced even more fine-tuned possibilities to control the visibility of one's information. The user may define lists (e.g. "*colleagues*", "*in-laws*"', and "*English-speaking friends*") and restrict the visibility of specific status updates, images or other information to only certain lists.

Data Collection

The empirical data was collected by a student at the Helsinki School of Economics (Helsinki, Finland) as part of her Master's thesis project. A web questionnaire was a natural choice because of research subject: users' behavior on the Internet. The main focus was on users' information disclosing in profiles, users' privacy and security concerns and their awareness of privacy on Facebook. The questionnaire items 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) demographic and background information; 2) Respondent's personals information and friends on Facebook; 3) Respondent's privacy controlling and settings; 4) Respondent's privacy and security concerns; 5) Respondent's awareness of Facebook Privacy Policy; and, 6) open feedback question (See Appendix for the full questionnaire).

160 Facebook users (contacts of the data collecting student) 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. Additionally, a convenience sample of 20 people (also contacts of the data collecting student) was used to ask people to answer the questionnaire via e-mail. Also all of these people were Facebook users, but usually logged in to Facebook only occasionally. These users had the possibility to forward the invitation, too. Using the snowball effect, a total number 210 acceptable responses were received.

FINDINGS

We will first introduce the sample and the background information of the respondents. We then present the respondents' information disclosing behavior in their Facebook profiles and discuss their privacy concerns and the awareness of privacy protection. Finally, some findings on privacy behavior are discussed.

Total number of 210 people responded to the questionnaire. Of these 56 % were female, 43 % male, and 1 % did not disclose their gender. Most (88%) of the respondents were under 30 years old but over 18 years. A large proportion (74%) of the respondents were students, more than half of them at the Helsinki School of Economics.

At the time of the data collection, Facebook was a fairly new phenomenon, also in Finland. 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 it easier to keep in touch*" (60 % had check this option). "*To find classmates*", "*Everyone I know is on Facebook*", and "*to network in general*" were also common reasons to join Facebook. In other words, networking and communication were the main reasons to create a Facebook profile and, in effect, to start disclosing information. This is in line with other studies (e.g. Dwyer et al., 2007; Ross et al., 2009) in the US context.

The respondents' number of friends varied a lot: 17 % have 50 or less, while 9 % have more than 350 friends. Most often, the respondents had reinforced their existing strong connections by inviting their "*close friends*" (92%) or "*friends*" (96%) to connect via Facebook. However, well more than half (65%) of the respondents had also invited people they "*just know*", as well as people they had only met once (12%), and even people whom they had not met at all (3%) as their Facebook Friends. Similar figures were true for accepting invitations from others.

All of the respondents logged into Facebook at least once a week, 86 % once or more than once a day. Slightly over half (55 %) of all respondents updated

their "*status*" once a week or more than once a week, while 23 % of respondents never updated their status on Facebook.

Information Disclosing

The respondents shared a large amount of information about themselves on Facebook. Only two respondents of 210 informed that they did not use their real names in the service. Almost all respondents (98 %) had a profile picture on their profiles, and most (more than 80 %) had included information about their hometown, date of birth, e-mail address and education details. 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

The general rule seemed 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 disclosed 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 had allowed access only to their friends (63%). Still, there were many (34%) who kept their profiles open to all the users part of the same network. There was no significant 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.

Privacy protection

It seems that the respondents were, to a slight degree, worried about their privacy when using the Internet. Also having one's credit card number stolen in the Internet seems to have brought concerns. Nevertheless, overall the respondents seemed rather trust the other Internet users, even though they thought that an identity theft could be a real privacy risk. The respondents were also fairly familiar with the concepts of data protection and security while using the Internet in general (see Table 2.).

Table 2: Privacy and data security concerns related to Internet 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 a scale of 1-7 (1 = strongly disagree, 7= strongly agree)

Results of privacy concerns on Facebook reveal that the respondents did not have notable concerns about privacy and data security while using Facebook, but rather felt comfortable about, for instance, writing to their Friends' walls (see Table 3.).

Table 3: Privacy and data security concerns related to 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 a scale of 1-7 (1 = strongly disagree, 7= strongly agree)

Overall, the respondents seemed to be more worried about privacy issues related to the Internet in general, than as related to Facebook in particular. This could be interpreted so that Internet was seen as the "great unknown", something rather vague with a number of both readily identified as well more unidentified risks, while Facebook, a platform shared with friends or "Friends" does not pose so many threats. This is supported by the fact that by and large, the respondents seemed to trust Facebook with their private information. Majority of the users (75%) claimed to know who can see their Facebook profile, while the rest (29 %) either did not know or were 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 %) were aware that the privacy settings can be modified, and the majority (84 %) said to have done so (see Table 5). Also, the respondents claimed to be knowledgeable about the fact that without modifying their privacy settings, their profile would be visible to the members of all new networks they join in.

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 was not as well acknowledged (see Table 6): over half (55 %) of the respondents did not know that if he or she adds an application, the developer of the application has a right to access the user's information. Furthermore, the majority (73 %) was not aware, that Facebook could, according to the 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 organizations 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 had read the Facebook privacy policy, and even fewer (15 %) had 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 said to have read the Facebook privacy policy, were not aware of Facebook's right to share their information with third parties. Whether this means that the privacy policy has been read in a cursory manner, at best, or whether the respondents do not want to admit not having reading it is difficult to say.

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, and commented along the lines of "*I will be more careful in the future*" and "*I certainly will now adjust my privacy settings*". As many as one in ten of all respondents mentioned specifically the Facebook add-on applications, and admitted not having realized the information access they have unwittingly granted to third parties. This indicates that increasing awareness of privacy can and will affect the user behavior: clear and compact information about privacy issues, features and practices makes users think about privacy and can result in more careful behavior in online environment.

DISCUSSION

Online social networking offers new opportunities for interaction and communication, first and foremost to individuals, but increasingly also to companies and other organizations, as well. Online communities present an easy and inexpensive way to maintain already existing relationships, form new ones and present oneself to others and communicate with them. In organizational context, SNS are seen to offer novel opportunities for customer relationship management (see e.g. Gallaugher & Ransbotham, 2010). However, the increasing number of different social networking services and activities conducted on them also gives rise to range of privacy concerns and risks.

As our study shows, users of the world's largest SNS, Facebook, seem to disclose a large amount of information about themselves to a large amount of both strong and weak connections, sometimes to people totally strangers to them. As in most similar studies (e.g. Ross et al., 2009), our subjects were mostly young adults and students. They did not have any significant privacy concerns, even though they claimed to be fairly aware of the related privacy risks. Whether more mature Facebook users share this fairly relaxed attitude towards privacy risks or not, remains a question for future research. Overall, the privacy risks were perceived to be smaller on Facebook than on the Internet in general, probably because Internet is seen as 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 more or less active users of Facebook, also that remains as a topic for future research.

The main implication of our study is that privacy policies are of central importance. This is not only because they inform the users about how their private information can be processed and utilized, but also because they partly define consent that the users agree to, when they add their private information into the service. Earlier studies (e.g. Acquisti & Gross, 2006; Gross & Acquisti, 2005; Jones & Soltren, 2005) have shown that privacy policies and the terms of use just do not get the attention of the users, and this was true to our survey respondents, as well. There could be several explanations for this: it is perceived to take too much effort to read them, they are difficult to comprehend, or the users trust the service provider so much that they feel they do not need to read policies.

Nevertheless, as our study shows, even reading the privacy policy does not guarantee increased awareness of service provider's privacy protection practices. Most of our respondents were – or claimed to be – aware of Facebook's privacy features and said to have also used them. However, default privacy settings of a SNS can seem confusing and some particular actions, for instance, joining a new network, might change settings without users realizing it.

SUMMARY AND CONCLUSIONS

In this paper, we have reviewed earlier research on privacy issues related to social network services, 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. Although our data was collected five years ago and some changes in the privacy policies of various SNS, including Facebook, have been made along the technological developments, we are confident that our findings are still relevant and have implications both to researchers as well as practitioners. Some studies (e.g. Boyd & Hargittai, 2010) have shown that user behavior is changing, at the latest with personally experienced privacy invasions (Debatin et al., 2009). However, the change is slow.

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, a number of issues are not fully understood by the users, who might even appear to behave irrationally. Privacy is a complex concept and, as such, difficult to understand. With the proliferation in the variety and number of different social media tools and services, including new functionalities brought about with location information, there are also an increasing number of different factors that affect privacy attitudes and behavior. Hence, more research into privacy awareness and related behavior on social network services is clearly called for.

ACKNOWLEDGMENTS

We are grateful to M.Sc. (Econ.) Marjaana Hovi, who conducted the web survey and collected the data used in this study. An earlier version of this paper was presented at the 22nd Bled eConference (Tuunainen et al., 2009).

REFERENCES

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

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

Boyd, d.m., and Ellison, N. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210-230.

Boyd, d. & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, 15, 8-2.

Brooks, G. (2007). Secret society., *New Media Age*, 13 December, 10.

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

Debatin, B., Lovejoy, J.P., Horn, A-K. & Hughes, B.N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communicatio,*. 15, 83-108.

Dinev, T. & Hart, P. (2006). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce*, 10 (2), 7-29.

Donath, J. (2007). Signals in social supernets. *Journal of Computer-Mediated Communication*, 13(1), 231-251.

Dwyer, C. (2007). 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,.

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

Gallaugher, J. and Ransbotham, S. (2010). Social Media and Customer Dialog Management at Starbucks. *MIS Quarterly Exec*utive, 9(4), 197-212.

German Federal and State Data Protection Commissioners (1997). 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.

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. (2007). 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 (2005). Information Revelation and Privacy in Online Social Networks. In the *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, 71 – 80.

Jones, H., and Soltren, J.H. (2005). Facebook: Threats to Privacy, MIT, USA.

Kosta, E. and Dumortier, J. (2008) 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", 2 (3), 276-288.

Lampe C., Ellison N., and Steinfield C.A. (2007). 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, 435 – 444.

Lampinen, A., Lehtinen, V., Lehmuskallio, A., Tamminen, S. (2011). We're in It Together: Interpersonal Management of Disclosure in Social Network Services. In the *Proceedings of CHI 2011*, Vancouver, Canada, May 7–12.

Lampinen, A., Tamminen, S., & Oulasvirta, A. (2009). All my people right here, right now: Management of group co-presence on a social networking site", In *the Proceedings of GROUP '09. ACM*, New York, May 10-13.

Lehmuskallio, A. (2009). A photo is not an extension of me, it's plain surface: Views of users of a Web 2.0 photo-sharing site on photos and privacy. *SPIEL: Siegener Periodicum zur Internationalen Empirischen Literaturwissenschaft*, 26, 1.

Pitkänen, O. (2006). Technology-Based Research Agenda on the Data Protection Law., In the Proceedings of *LawTech 2006*, Cambridge, MA, USA. October 9 – 11.

Ross, G., Orr, E.S., Arseneault, J.M. Simmering, M.G. & Orr, R. (2009). Personality and motivations associated with Facebook use. *Computers in Human Behavior*, 25, 578-586.

Tow, W.N-F.H., Dell, P., Venable, J.R. (2008), Understanding Information Disclosure Behaviour in Australian Facebook Users. Om proceedings of the *19th Australasian Conference on Information Systems (ACIS) 2008*, Christchurch, New Zealand, December 3-5.

Tuunainen, V., Pitkänen, O., Hovi., M. (2009). Users' Awareness of Privacy on Online Social Networking Sites – Case Facebook. In the proceedings of the 22nd Bled eConference. Bled, Slovinia, June 14-17.

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

APPENDIX: SURVEY INSTRUMENT

Background Information

1) **Age**:
   - Under 18
   - 18-21
   - 22-25
   - 26-29
   - 30-34
   - 35-38
   - Over than 38
2) **Gender**:
   - Female
   - Male
3) **How related to HSE**?
   - HSE student, class (1-n):
   - Exchange student at HSE
   - Student at other university
   - Student at other school
   - HSE alumni
   - Other
4) **How long you have had a profile on Facebook**? (Months)
5) **Check all of the following reasons for joining Facebook that apply to you**:

- A friend suggested it
- "Everyone I know is on Facebook"
- Find classmates
- Find people who share my interests
- Make easier to keep in touch
- Show information about myself /advertise myself
- Help to express my opinions
- Get to know more people
- Find dates
- Find jobs
- To network in general
- Other reason

Personal Information and Friends

6) **How often do you log in to Facebook**? (on avarage)

- More than once a day
- Once a day
- More than once a week
- jOnce a week
- Less than once a week
- Less than once a month

7) **Have you used Facebook with your mobile phone**? (Yes / No)

8) **Check all of the following options what you normally do when you log in to Facebook**:

- Update my profile information
- Upload new photos
- Look at profiles and photos of my friends
- Look for more friends to add my friend list
- Contact new people
- Have fun with my applications
- Send private messages to my friends
- Send messages to my friends' walls
- Add new applications
- Other, what?

9) **Check all the following information you have on your profile**:

- Real name
- Profile picture
- Birthday

- Hometown
- Sexual orientation (interested in)
- Political views
- Relationship status
- Partner's name
- E-mail address
- Contact phone number
- Street address
- Website
- Education info
- Activities / interests
- Favorite music, movies etc.
- Photos of you
- Photos of your friends

10) **How often you update your status (where are you, what are you doing etc.**)?

- More than once a week
- Once a week
- More than once a month
- Once a month
- Never

11) **Have you joined any Networks**?

- HSE-network
- Finland-network
- Other
- No

12) **How many groups you have joined**?

- 0
- 1-5
- 6-10
- 11-15
- More than 15

13) **How many friends you have on Facebook** (friend list)?

- 0-50
- 51-100
- 101-150
- 151-200
- 201-250
- 251-300

- 301-350
- More than 350

14) **What type of friends have you asked to be your friend**? (Check all options)

- Close friends
- Friends
- People you just known
- People you have just met once
- People you haven't met

15) **What type of friends have you accepted requests to be your friend**? (Check all options)

- Close friends
- Friends
- People you just known
- People you have just met once
- People you haven't met

16) **Have you ever looked at a profile or photos of someone complete stranger to you**? (Yes / No)

Privacy Control and Privacy Setting

17) **Do you know who can see your profile and the information in it**? (Yes / No / I am not sure)

18) **Are you aware that you can change your privacy settings**? If your answer is "no", you can skip next three questions (numbers 19-21). (Yes / No)

19) **Have you ever used your privacy setting**? If your answer is "no", you can skip next two questions (numbers 20-21). (Yes / No)

20) **Who can see your profile and your information**? Please check following options: (My networks and my friends / Only my friends / Only me or no one / I don't know or remember)

- Profile
- Tagged photos of you
- Online status
- Friends
- Wall
- Contact e-mail

21) **What can people (who can't see your profile but can find you) do with your search result**?

- See your picture

- Send you a message
- Poke you
- Add you as a friend
- View your friend list
- I don't know / remember

22) **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**? (Yes / No)

Privacy and Data Security Concerns

23) **Privacy and data security concerns in general**
(On a scale of 1 – 7 ((1= strongly disagree, 7= strongly agree))

1. I worry about my privacy and data security while using the internet
2. 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
3. I worry about people online not being who they say they are
4. I feel that identity theft could be real privacy risk
5. 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
6. I am familiar with data protection and securing while using the internet in general

24) **Privacy and data security concerns on Facebook**
(On a scale of 1 – 7 ((1= strongly disagree, 7= strongly agree))

1. I worry about my privacy and data security while using Facebook
2. I feel that the privacy of my personal information is protected by Facebook
3. I trust that Facebook will not use my personal information for any other purpose
4. I feel comfortable writing messages on my friends' walls
5. I worry that I will be embarassed by wrong information others post about me on Facebook

The Facebook Privacy Policy

25) **Have you read the Facebook privacy policy**? (Yes / No)
26) **Have you read the Facebook terms of use**? (Yes / No)
27) **Are you aware that Facebook can share your information with people or organisations outside of Facebook for marketing purpose as their privacy policy**? (Yes / No)

28) **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**? (Yes / No)
29) **Do you think this questionnaire affects your behavior on Facebook anyhow**? (Yes / No)
30) **If yes, how**?
31) **Open feedback on the questionnaire, survey or subject** (in English or in Finnish):

AUTHOR BIOGRAPHY

Olli Pitkänen is a senior research scientist, research group leader, and a docent at Aalto University. He holds a doctorate in information technology, a master's degree in software engineering, and a master's degree in laws. He has worked as a researcher and a teacher at Aalto University, at Helsinki University of Technology and at Helsinki Institute for Information Technology HIIT (http://www.hiit.fi) since 1993. Prior to academia he had worked as a software engineer and practiced law in the private sector. He has also been a member of the board in several IT companies. In 1999-2001 and 2003, he was a visiting scholar at University of California, Berkeley. He has also been a visitor at The Interdisciplinary Centre for Law and Information & Communication Technology, K.U. Leuven, Belgium. His research interests include legal, societal, and ethical issues related to future media, digital services, and information and communication technologies (ICT).

Virpi Kristiina Tuunainen is professor of information systems science at the Department of Information and Service Economy of Aalto University School of Economics, and director of Aalto University Service Factory. Her current research focuses on ICT enabled or enhanced services, electronic and mobile business models, and economics of IS. Her work has appeared in journals, such as, MIS Quarterly, Communications of the ACM, Journal of Management Information Systems, Journal of Strategic Information Systems, Information & Management and Information Society, and in conferences, such as, HICSS and ECIS.