Privacy Protection Issues in Social Networking Sites

Ai Ho, Abdou Maiga, Esma Aïmeur
Département d'informatique et de recherche opérationnelle
Université de Montréal
Montreal, Canada
{hothitha, maigaabd, aimeur}@iro.umontreal.ca

***Abstract*— Social Networking Sites (SNS) have become very popular during the past few years, as they allow users to both express their individuality and meet people with similar interests. Nonetheless, there are also many potential threats to privacy associated with these SNS such as identity theft and disclosure of sensitive information. However, many users still are not aware of these threats and the privacy settings provided by SNS are not flexible enough to protect user data. In addition, users do not have any control over what others reveal about them. As such, we conduct a preliminary study which examines the privacy protection issues on Social Networking Sites (SNS) such as MySpace, Facebook and LinkedIn. Based on this study, we identify three privacy problems in SNS and propose a *Privacy Framework* as a foundation to cope with these problems.**

Keywords: Social networking site, privacy, privacy framework.

I. INTRODUCTION

Advances in Information Technology have brought out many changes in the nature of communication and socialization. A few years ago, blogs, forums, instant messaging, podcasts, online photo albums bloomed on the Internet. Nowadays, all these media are brought together in Social Networking Sites (SNS). An SNS is a website that provides a virtual community for people interested in a particular subject or just to "hang out" together (Computer Desktop Encyclopedia[1]). According to Bob Ivins, vice president of *comScore*.com, "*social networking is not a fad but rather an activity that is being woven into the very fabric of the global Internet.*" On the expansion of social networking across the globe, several major SNS such as *MySpace* (www.myspace.com), *Facebook* (www.facebook.com) and *Hi5* (www.hi5.com) have experienced dramatic growth since 2006. *LinkedIn* (www.linkedin.com) is also a well-known online network with more than 25 million experienced professionals from around the world, representing 150 industries.

According to *Alexa* (www.alexa.com), seven of the top 20 most visited Web sites in the world are social-networking sites, such as MySpace, Facebook, *Orkut* (www.orkut.com), or contain significant social networking components (e.g. sharing videos, blogs...) like *YouTube* (www.youtube.com) or *Blogger* (www.blogger.com).

The rapid growth of SNS in recent years indicates that they are now a mainstream communications technology for many people. The people who use social networking sites see them as a fun and easy leisure activity. Through SNS, users can keep in touch with friends and family, especially with people they do not see on a regular basis, find old friends, contact friends of friends, and even contact people they haven't met before. By extending their social circle, users have the opportunity to communicate with people who have the same interests. However, since the reputation of these SNS has been tarnished by a number of incidents in news media, such as the massive worldwide *spam* campaign in *Quechup* [1], *sexual predators, stalkers, child molesters...* SNS users have reasons to be concerned about their privacy. For example, starting from September 2008, Facebook can no longer be accessed from desktop computers with a wired connection to the Concordia University network. This university is worried that the continuing reliability of its network could be compromised because of spam, viruses and leaks of confidential information related to Facebook use [2].

We group the privacy risks in SNS into three categories: *Security risks* (identity theft, phishing...), *Reputation and Credibility risks* (for example, companies do background checks on prospective employees [3, 4] or the case where Canadian border guards posted inappropriate and unprofessional material on Facebook [5]) and *Profiling risks* (spam, unsolicited collection of user data...).

Although SNS provide some mechanisms (privacy settings, block users...) to protect users against these risks, these mechanisms are insufficient.

The top and foremost privacy problem is that SNS do not inform users of the dangers of divulging their personal information. Although privacy and safety issues are the subject of much discussion in the media, according to [6], these issues still did not emerge as '*top of mind*' for most users of SNS. They are seemingly unwilling to consider that there could be a more serious side to their activities on SNS.

[1] www.answers.com/topic/social-networking-site

Even if they want to protect their privacy, with too much data and too many friends, it is very difficult for users to control who can see what on their profile pages.

The second problem is that Privacy tools in SNS are not flexible enough to protect user data**.** Most SNS only allow users to make their data either public (available for everyone) or private (available only for Friends) the whole profile but not every part of it. Facebook is one of the few SNS that provide very detailed privacy settings. However, the current Facebook privacy interface is too complex to most normal users.

The third problem is that when users of SNS can control access to their own profile, they cannot control what others reveal about them. It is possible for information to be passed on without one's consent. For instance, a user can upload an embarrassing photo of a friend; this photo can also be *tagged* directly to a friend's profile.

Moreover, the service providers of SNS have unlimited access to users' data. With this enormous amount of information, there are many commercial opportunities for businesses on social networking sites. Marketers who target specific kind of consumers can use stated, personal information gathered from SNS for purposes other than what users intend. *eMarketer*.com reported that $900 million dollars were spent in the United States on social network advertising in 2007 and that the amount will nearly triple to $2.5 billion by 2011.

Although there are some proposed solutions [7, 8], they can not entirely fix the privacy problems. Therefore, we conduct a preliminary study to examine the usage and privacy concerns in SNS. Based on this study, we introduce a *Privacy Framework* for SNS. First, the user data is divided into groups and categorized based on its privacy risk and its importance to the users. We also introduce four groups of people who can have access to user data. Secondly, we adapt the four *privacy levels* defined for e-commerce by our team [9] to the context of SNS.

II. METHODOLOGY

Our preliminary study is based on an online survey that lasted for ten days with 200 participants.

A. *Recruiting methods*

Most of the participants of the survey are students and professionals in Canada. During the survey, there were 200 participants, where 71.5% (144) had at least one SNS account.

B. *Survey design*

The survey questionnaire contained twenty eight questions: *demographic questions* (age, occupation, gender, etc.), *SNS usage questions* (purposes for joining SNS, profile information, friends, etc.) and *privacy concern* questions such as intellectual copyrights and unauthorized data access. Some of these questions are inspired from [10].
The survey is available online in two versions: http://spreadsheets.google.com/viewform?key=p7AZRICDTMB4yGleAbYOwOA&hl=en in English and http://spreadsheets.google.com/viewform?key=p7AZRICDTMB5J8EhxCVkFbg in French.

C. *Statistical analysis*

The results were analyzed using SPSS 16. In order to assure the validity of the results we performed a number of statistical tests: Chi square one-sample test and K-mean Cluster Analysis.

III. PRIVACY ISSUES IN SNS

Privacy risks such as Security, Profiling, Reputation and Credibility are much more noticeable in SNS than other media such as personal websites, blogs, etc. This is because SNS provide a sense of intimacy created by being among online Friends. With the motivation to communicate and maintain relationships, the amount of information revealed willingly by the user is much greater than what he would have on other media. Moreover, SNS make it extremely easy to upload many different forms of personal information, such as age, contact information (including home address and telephone numbers), photos, sexual orientation, and music preferences. In a survey of [11], 91% of Facebook participants and 62% of MySpace participants use their real name to identify themselves. Our survey also has similar results: 65% of the participants currently share photos of themselves on the SNS. Moreover, 94% of them are ready to provide some or all real personal data (name, email...) on the SNS if they are required.

In order to protect user privacy, all SNS provide some level of privacy control that allows users to control *who* sees *what* in their profile. The most common privacy features are: *Profile privacy* (control who can view the user profile and personal information), *Application privacy* (control what information is available to installed applications), *News Feed privacy* (control what user stories get published in the feeds). Facebook also provides Search privacy features that control who can search for the user and how he can be contacted. The Profile views settings in LinkedIn help the user control what type of information about him appears in other LinkedIn users' "Who's viewed my profile" list. Another noticeable privacy control in Facebook is that the user is given a brief notice when others tag images with that user's name. The user also has the option of removing the tag.

However, these tools are not efficient enough to protect user privacy on SNS.

Problem 1: The first and foremost privacy issue in SNS is that these SNS do not make users aware of the dangers of divulging their personal information.

Most SNS only focus on the connection and interaction between users. They describe themselves as "an online community that lets you meet your friends' friends" or "a social utility that connects you with the people around you". Social networking sites make it extremely easy to provide different forms of personal information (age, hobbies, religions, music, blog, video...) but do not adequately educate users about the risks of disclosing their information.

TABLE 1: DO SNS PROVIDERS WARN YOU ABOUT THE RISK OF DIVULGING YOUR PERSONAL INFORMATION ONLINE?
(p=0.001 Chi square one-sample test)

	Observed N	Expected N	Residual	Percentage
Yes, these warnings are very useful	31	46.7	-15.7	22%
I am not sure	67	46.7	20.3	47%
No, I have never seen these warning	42	46.7	-4.7	29%
Missing answers	4			3%
Total	144			

Based on the survey, we can safely conclude that most SNS users (76%) do not know about privacy warnings provided by SNS providers (see Table 1).

In fact, safety tips appear at the end of MySpace's webpage, and then all useful information is buried under lots of banner ads. According to [7] Facebook users do have difficulty understanding the existing privacy settings. Due to the complexity of the current Facebook privacy interface, only those who are very motivated will make the effort to adjust their settings.

In most SNS, privacy settings are defaulted to share users' personal information. If users wish to restrict the information that they share, they must opt-out most of the sharing settings. Moreover, users are not automatically directed to Privacy settings page upon registering and creating a profile.

As a result, Ofcom's qualitative research on social networking sites [6] showed that privacy and safety issues did not emerge as 'top of mind' for the majority of users. A Facebook demographics study [12] of Carnegie Mellon University students found that 88.8% disclosed their full birth date and gender to their network, and 45.8% also posted their current residence. Privacy concerns are largely being ignored (sometimes unknowingly) in the current rush to online lifecasting [13]. While small pieces of information seem to be harmless, simple combinations like date of birth and zip code can be used to identify a person and provide the basis for gathering more information about him.

Moreover, personal information, once publicly posted on the Internet, can come back to haunt users later. Once something appears on the Internet, it's almost impossible to remove. If the user posted a reputational damaging photo of himself on a SNS and removed it later, there is a chance that someone had already seen it and downloaded it to their computer. Companies now routinely use search engines to do their background checks on prospective employees and also often review SNS where students post "provocative comments about drinking, recreational drug uses, etc. in what some mistakenly believe is relative privacy." Business and governmental organizations also worry about their employees giving out proprietary information or posting content that can jeopardize their reputation.

Problem 2: Privacy Tools in SNS are not flexible enough to protect user data.

According to a small survey of [14], most SNS employ the Friends model as an access control mechanism. Some SNS only offer basic access control which means that the user is allowed to make public or private the whole profile but not specific parts of it.

In our survey, even though 84% of the participants use the privacy settings to protect all or some of their information, there are 10% that do not know how to use these settings. Moreover, only 42% of the participants use the spam blocking feature and succeeded. The rest do not know how to block spam or think that the feature does not work.

Facebook is one of the few SNS that provide detailed privacy settings. However, as the current Facebook privacy interface is too complex, most users will choose the simpler way: set the entire profile to only be viewable by friends, as this could be done from a single menu without digging into the details of the rest of the privacy settings [8]. Consequently, user's profiles were either entirely public, or entirely private.

Problem 3: The users cannot control what others may reveal about them.

Friends can be untrustworthy. Users can control information in their profile but not in their Friends' profile. For example, Alex posted a photo of himself and his friends drinking in a classroom. He only allowed his Friend Bob to see it. Bob put a comment for this photo: "Wow, Alex, you got drunk at school", and all Bob's Friends can see this comment because they are subscribed to Bob's Activity Feed.

Another problem is tagging. As SNS allow users to tag other users in photo, it is not only possible to see the photos in a user's album but also those published by others that are tagged with his name.

Some SNS such as Facebook let users remove tags pointed to them at will, nonetheless if someone has already seen the tag, it is too late and the damage is done.

In our survey, even though 58% of the participants are very concerned that other people might reveal their real identity and personal information online without their consent, 26% are still ready to disclose photos and comments of their friends.

Users also have no control over *third parties*. Users cannot add an application to their profile without granting it permission to access all their public and private data. A simple application Send a Rose which allows a user to send roses to his friends requires unnecessary full access to the user's data.

This increases the risk of having "attractive" applications that spy on users and collect their data.

Facebook additionally gives third parties second-degree access: when Alex installs a third party application, it can also request information about Alex's friends and fellow

network members. However, according to [8], most applications do not need the extensive personal information that is available to them, in fact only 9.3% of Facebook applications require access to private data.

Moreover, users have no control over how third party companies (such as marketers) use their personal information. Due to the fact that most income of SNS is from advertising, these SNS allow merchants and third parties to take advantage of user information without their agreement. Companies such as Coke, Apple Computer and Proctor & Gamble are using social networking sites as promotional tools.

Indeed, businesses can use the Social Ads tool in Facebook to target their advertisements based on criteria related to location, sex, age, education status, workplace, political views…

Last but not least, the Service providers of SNS have too much control over user information.

Like many websites that collect user information, all SNS have privacy policies. A privacy policy is a disclaimer informing users about how the SNS deals with a user's personal information. By accepting the terms of the policy, the user volunteers to relinquish some known right or privilege they may have. A user cannot know if the SNS is respecting its privacy policy.

Moreover, these policies may be changed by the SNS anytime. The SNS are also unclear about the terms by which user details are shared with third parties. Facebook, MySpace and Friendster affirm that the user can choose to share information with marketers through sponsored groups or other on-site offers, such as competitions or sweepstakes. As a result, even if the users apply the strictest privacy settings, they still do not have total control over their personal information. According to Facebook's Terms of Use, the user uploaded content becomes the property of that site.

These SNS also collect and store other data about users such as personal interests, gender, age, education and occupation, IP address… in order to "improve the website services".

Even after users delete their profile, all of their personal information that was collected over the course of their membership is retained for a period of time. In Facebook, users are simply informed that account reactivation is possible in the future.

In our study, more than 60% of participants are concerned that the SNS provider might disclose their information without their consent (see Table 2)

TABLE 2: ARE YOU CONCERNED THAT THE SNS PROVIDER MIGHT DIVULGE YOUR INFORMATION TO OTHER PARTIES WITHOUT YOUR EXPLICIT CONSENT?
($P<0.05$)

Answers (from 1 to 5)	Frequency	Percentage	Valid Percentage	Cumulative Percentage
1 (Not at all)	11	7.6	7.7	7.7
2 (Somewhat)	19	13.2	13.4	21.1
3 (Neutral)	12	8.3	8.5	29.6
4 (Much)	46	31.9	32.4	62
5 (Very much)	54	37.5	38	100
Responses	142	98.6	100	
Missing	2	1.4		
Total	144	100		

IV. EXISTING PARTIAL SOLUTION

Since the beginning of SNS, privacy has become a primary concern. In one of the first academic studies of privacy and SNS, [15] analyzed 4,000 Carnegie Mellon University Facebook profiles, evaluated the amount of information they disclose, and studied their usage of the site's privacy settings. This survey also highlighted potential attacks on various aspects of user privacy such as stalking, re-identification and identity theft. [15] shows that there is often a difference between students' desire to protect privacy and their behaviours. This is mostly because users are unaware of the public nature of the Internet. However, user awareness has been changing dramatically. In 2005, only 0.06% of more than 4000 users at Carnegie Mellon University changed the default profile visibility in Facebook [15]. In 2008, in a survey of the Office of Communication (United Kingdom) [6]. 48% of the participants reported that their profile was able to be seen only by their Friends.

There are also other researchers that focus on the identification of privacy risks in SNS. These authors also propose some guidelines to protect user privacy.

Lipford *et al.* [7] examine the role of interface usability in current privacy settings on Facebook, then propose a prototype to help user feel more at ease with these settings. However, this prototype only slightly improves the user interface without really changing the privacy settings behind. The users may understand how privacy settings work, but not why they need to use them and what they should do. The prototype does not educate users of the privacy risks behind social networking activities.

Felt and Evans [8] study 150 popular Facebook applications and address the privacy risks associated with social networking APIs (Facebook API and Open Social). The authors propose a privacy-by-proxy designed for a privacy-preserving API to solve these risks. However, applications using user's private data do not work well with this approach because processing time is too long. The approach does not give a complete solution for all the privacy risks in SNS.

To the best of our knowledge, the current researches do not solve all the privacy risks in SNS because they all are built on the existing SNS. The focus of current SNS is interaction and sharing information between users without much concern about user privacy. Thus, we need to build a privacy foundation for social networking and create a new SNS based on this foundation.

V. PRIVACY FRAMEWORK

The role of the Privacy Framework is to provide a foundation for SNS in which privacy issues can be addressed. In this part, we categorize user data, user privacy concerns and profile viewers. Based on these categorizations, we adapt the privacy levels [9] and tracking levels [16, 17] to the context of SNS.

A. User data

In our study, users list some type of information that they would place on their profile (see Figure 1).

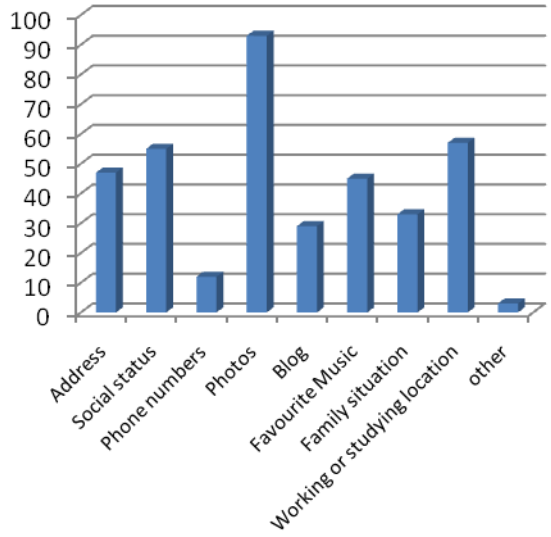

Figure 1: Information on user profile

Based on the survey, we categorize user data into 5 groups: *Identity, Demographic profile, Activity, Social Network,* and *Added content.*

Identity refers to information that makes it possible to determine physically who the user is. This includes information such as name, address or telephone number.

Demographic refers to the demographic characteristics of the user, such as age, gender, weight, race, and/ or political view.

Activity lists all the activities that users perform within the SNS, for instance: adding new Friends, writing a comment in profile of other users, and/ or changing their status. The Activity data is automatically collected by the SNS provider and is displayed in News Feed format.

Social Network refers to the relationships of users in SNS, such as who are their Friends or the groups they subscribed to.

Added content is all the information that users put on their profile page, including blog, photos, music or video clips.

B. User privacy concern

In order to evaluate how much SNS users prize their online privacy, we perform the K-mean Cluster Analysis on the questions about user privacy concerns, such as: Are you concerned that the information you displayed specifically to someone may be inappropriately forwarded to others?

The K-CA run with k=2 resulted in two user groups with 92 and 52 members respectively. In Table 3 we can see the contributions on each variable to the formation of the groups. Members of Group 1 (64%) consider online privacy a very important factor. In contrast, the members in Group 2 (36%) seem less concerned about privacy with ratings below average.

TABLE 3: FINAL CLUSTER

Question (1: not at all, 5: very much)	Cluster	
	G1	G2
	Average	Average
Are you concerned that the information you displayed specifically to someone may be inappropriately forwarded to others?	4	3
Are you concerned that the photos shown in your profile may be downloaded and transmitted by others?	4	3
Are you concerned that the people you only know online are not who they say they are?	4	2
Are you concerned that other people might reveal your real identity and personal information online without your consent?	4	3
Are you concerned that your intellectual properties might be copied or abused by others? (For example: articles, photos and ideas)	4	2
Are you concerned about online identity theft, profiling or phishing?	4	2
Are you concerned that the SNS provider might divulge your information to other parties without your explicit consent?	4	3

Since different users have different privacy concerns for each piece of information, we propose four **Privacy settings** for user data according to impact on user privacy: *Healthy, Harmless, Harmful* and *Poisonous*.

Healthy data is general information about users such as nick name, usual hobbies, landscape photos, and music video clips. Specifically, if an unauthorized person accesses this data, it cannot be tracked back to the user. The user can confidently share this data without any privacy concern.

Harmless data contains the user's demographic profile, such as gender, religion, age groups, and political views.

Specifically, the disclosure of harmless data does not create either *Security* risks or *Reputation and Credibility* risks. However, it can lead to *Profiling* since some marketing companies can collect this data and build a profile of the user.

Harmful data refers to inappropriate photos or blog entry that may damage the user's reputation, for example a photo of Alex in his job uniform smoking pot. This data can damage the *Reputation and Credibility* of the user.

Poisonous data contains information that may cause *Security* risks such as the user's financial information, name, address, SIN (Social Insurance Number)... Cyber criminals can use this data for identity theft purposes.

C. Profile Viewers

These four Privacy settings: *Healthy, Harmless, Harmful* and *Poisonous* indicate to what extent the information disclosure can cause privacy risk to the user. Nonetheless, this categorization of user data is not sufficient by itself. Specifically, the level of security threats depends, not only on the type of data being disclosed, but also on the person to whom it is being disclosed. For instance, allowing your brother or sister to see your credit card information (Poisonous data) might not be as big as a risk, especially when you do trust them. As such, different Privacy levels for the various data are required.

In our study, most of users' online friends are real friends and real acquaintances. However, some of them (24.8%) are ready to become friends with strangers (see Figure 2).

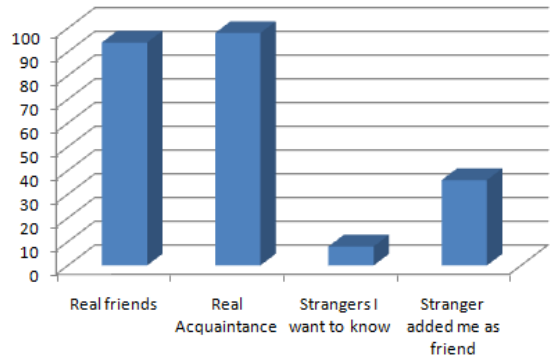

Figure 2: What kind of people do you have in your friend lists?

Thus, according to the intimacy and trust among users in SNS, we classify people who can see the user profile into four basic groups: *Best Friends, Normal Friends, Casual Friends*, and *Visitors.*

Best Friends are people that the user trusts enough to share nearly everything with. They often are best friends of the user in real life.

Normal Friends can be the user's family members, relatives or friends in real life.

Casual Friends usually are people about whom the user only knows a little. The user may only be acquainted with them online.

Visitors could be users or non-users of the SNS. They usually can only see the user's nickname or his avatar. They are not in the Friend list but they may be able to see user's avatar or some personal information such as name, age and location.

D. Privacy levels

Based on these four basic groups, we adapted the four levels of privacy in [9] to the context of SNS:

No Privacy: the user does not care about the privacy of his personal information. Everyone can see all his information on the SNS

Soft privacy: the user wants to keep his *Poisonous* data only for *Best Friends*. The *Visitors* are allowed to see *Harmless* and *Healthy* data of the user. The *Casual* and *Normal Friends* can access to all user data, except the *Poisonous* one.

Hard privacy: The *Normal Friends* still can access to *Harmful* data but the user put more limit on *Visitors* as they can only see the *Healthy* data and the *Casual Friends* only have access to *Harmless* and *Healthy data*.

Full privacy: the user does not allow *Visitors* to access his data. The *Poisonous* and *Harmful* data are restricted to *Best Friends* and the *Normal* and *Casual Friends* can access *Harmless* and *Healthy* data only.

Table 4 summarizes the access privileges of the four categories of *friends* to various groups of data, depending on the privacy level.

TABLE 4: PRIVACY LEVELS FOR SNS

	No Privacy	***Soft Privacy***	***Hard Privacy***	***Full Privacy***
Best Friends	All data	All data	All data	All data
Normal Friends		Harmful, Harmless and Healthy data	Harmful, Harmless, Healthy data	Harmless and Healthy data
Casual Friends			Harmless, Healthy data	Healthy data
Visitors		Harmless, Healthy data	Healthy data	No data

It is important to note that there is no real "Full Privacy" in SNS because the purpose of SNS is sharing information. If no one is allowed to see user data, there is no reason to use the SNS.

E. Tracking levels

Besides privacy levels, the user also worries about being tracked through profiles of other users on SNS. There are three possible ways of *Tracking* a user on SNS: following a profile link in a Friend list of a user, follow a name tag of a user, and reading information about a user in one of his Friends' profile. Consequently, we adapt the three Tracking levels defined by our team in [16, 17] for SNS (see **Table 5**)

Strong tracking: The user does not mind being tracked on SNS

Weak tracking: The user does not mind if his name appears on the Friend list but he does not want his Friends to put a tag on their Profile linking to his profile.

No tracking: The user does not want to be mentioned at all in his Friends' profile: no name, no tags, no photos.

TABLE 5: TRACKING LEVELS

	Strong tracking	***Weak Tracking***	***No tracking***
Best Friends	Tracking allowed	No tag	No information
Normal Friends			
Casual Friends			
Visitors			

Privacy settings and Privacy levels define an equilibrium between user privacy and the utility of SNS. Because the main reason of SNS is connecting people and sharing information, a SNS would be useless if users consider all their information harmful and do not want others to see it.

VI. IMPLEMENT PRIVACY FRAMEWORK

The proposed Privacy Framework is exhaustive and is able to cover all the possible case of privacy. However, normal users have to spend a lot of time, especially at the beginning, to understand and to configure their privacy settings.

Fortunately, the level of privacy risks of each user can be determined by his usual behaviours and attitudes on SNS. Ofcom's study points out five distinct prototypes of SNS users: *Alpha Socialisers*, *Attention Seekers, Followers, Faithfuls* and *Functionals* [6]. As users of each prototype have different notions of privacy and how they should conduct themselves on SNS, they are more susceptible to different kind of privacy risk.

Alpha Socialisers are people who use SNS to flirt, meet new people, and be entertained. They like to traverse Friend lists and put lots of comments on others' profiles and photos. As a result, their network and number of Friends are quite large but most of them are only Casual Friends. Alpha Socialisers may also give to Friends their contact details such as MSN address or phone number so they can communicate easily outside the SNS. These actions can lead to disclosure of personal information and *Security* risks.

Attention Seekers are people who crave attention and comments from others. To get attention, they often post lots of photos, primarily photos of themselves and Friends in "*suggestive poses, partying, drinking and portraying 'glamorous' lifestyles...*" [6]. Their network is quite extensible; nonetheless they tend to have active online connection with only a few Friends. Due to the large number of photos, the Attention Seekers are the most susceptible to *Reputation and Credibility* risks.

Followers are people who join SNS to keep up with what their peers are doing. They often browse through Friends' album, occasionally exchange comments and update their profile. Compared with Alpha Socialisers and Attention Seekers, users in this group are less likely to contact or meet people who they do not know. Consequently, most of their Friends are *Best Friends* and *Normal Friends*. There are many Followers on SNS, they have a moderate level of *Reputation and Credibility* risks as well as *Profiling* risks.

Faithfuls are people who typically use social networking sites to *rekindle old friendships*, often from school or university. They often leave their profile public so that old friends can find them on SNS. For them SNS are useful tools to strengthen existing offline networks rather than to create new, virtual ones. Due to the profile being public, the Faithfuls are easy victims of *Profiling* risks.

Functionals are a minority of people who tend to be single-minded in using SNS for a particular purpose, such as organizing parties, viewing photos, doing charity work... [6] reported that most of them were pestered to join SNS by friends who were more involved in the sites. They are occasional users and generally log on for short visits. These users also suffer from privacy risks because they don't spend the time to learn about privacy settings and just leave their profile opened by default.

Table 6 summarizes these five prototypes, their characteristics and the proposed privacy levels.

TABLE 6: TYPES OF SNS USERS

	Alpha Socialisers	***Attention Seekers***	***Followers***	***Faithfuls***	***Functionals***
Numbers of Friends	Many	Many	Medium	Medium	Several
Principal types of Friends	Casual Friends	Casual Friends	Normal Friends	Normal Friends	Casual Friends
Spending times	Usually	Nearly always	Often	Less than often	Occasionally
Data	Lots of Photos, Comments, Tags, Activity	Lots of Photos, Comments, Blog, Tags, Activity	Some photos, Comments, Activity	Some photos, Comments, Activity	n/a
Data type	Mostly Harmful	Mostly Harmful, Poisonous	Harmless	Harmless	Harmless
Privacy Risks	Security Reputation and Credibility	Security Reputation and Credibility	Reputation and Credibility Profiling	Profiling	Profiling
Proposed Privacy Level	**Soft Privacy No Tracking**	**Soft Privacy No Tracking**	**Hard Privacy No Tracking**	**Soft Privacy No Tracking**	**Hard Privacy Soft Tracking**

By asking users various simple questions such as "Why do you join SNS?" or "How often do you visit your page?" the framework would be able to classify them into appropriate prototype. Based on the characteristics of each prototype, we can propose to the user an appropriate privacy level that would give him enough freedom to do what he wants on SNS. For example, the main concern of a Faithful is to connect with old friends or distant relatives. Thus, he would be more comfortable with Soft Privacy, because with Healthy and Harmless data being public, it is easier for other users to find him on SNS. If the information provided by the user is not enough to build up a prototype, the framework will set the default Privacy level to the strictest one: Hard Privacy and Soft Tracking. Later, the user is able to customize the default level to make it more suitable to his situation.

This approach can help the user effortlessly determine their privacy level and tracking level. Moreover, he also is educated about all the potential risks of his future activities. That is the advantage of our Privacy Framework in comparison with other existing solutions.

VII. Conclusion and Future Works

Since their introduction, SNS (Social Networking Sites) such as MySpace, Facebook, Hi5 and LinkedIn have attracted millions of users and have become established places for keeping in contact with old acquaintances and meeting new ones. Because of the numerous interactions between users, there are large amounts of information circulating on the SNS.

As a consequence, huge quantities of user data, including personal information, pictures and videos continue to quickly fall into the hands of authorities, strangers, recruiters, and even the public at large. The existing solutions are not enough because the problems lie in the foundation of SNS: specifically, the current SNS focus on interaction and sharing information between users rather on user privacy. Recently, the September 2008 special issue of the *Scientific American* raised the question about the future of privacy in a Facebook age: "*Can we safeguard our information in a high-tech and insecure world?*" To answer this question, first of all we identify three main privacy problems in SNS: *lack of user awareness, the current privacy tools are not flexible enough* and *users have no control on what others reveal about them*. Secondly, we conduct a preliminary study including an online survey to examine the privacy protection issues in SNS. This survey included 200 participants. Even though the survey might not cover the whole spectrum of SNS users, its results further confirm the existence of these three privacy problems. Thirdly, we set up the *foundation* for privacy and introduce a *Privacy Framework* for SNS. Specifically, since privacy revolves around user data, we categorize user data, user privacy concerns as well as profile viewers into groups. Based on these categorizations, we present four privacy levels (No Privacy, Soft Privacy, Hard Privacy, Full Privacy) and three tracking levels (Strong Tracking, Weak Tracking and No Tracking). In order to help users choose the appropriate privacy levels, we also propose the default levels based on user purpose and behaviour in SNS. It is important to notice that Full Privacy is not recommended as this option conflicts with the main purpose of SNS: connecting people and sharing information.

Moreover, privacy comes with a price: users, especially the novice ones, have to invest considerable time and effort in order to protect their privacy. Thus, in the future, we intend to design and implement tools that offer users an easy and flexible way to specify and then communicate their privacy concerns to other users, third parties and SNS service provider. An extended survey is also necessary to validate the efficiency of our Privacy Framework to protect user privacy.

References

[1] C. Lake. *Quechup launches worldwide spam campaign* eConsultancy 2007 [cited 18.08.2008]; Available from: http://www.e-consultancy.com/news-blog/364182/social-network-launches-worldwide-spam-campaign.html.

[2] CBCNews. *Concordia bans Facebook access on campus computers* 2008 [cited 28-09-2008]; Available from: http://www.cbc.ca/consumer/story/2008/09/17/mtl-concordiafacebook0917.html.

[3] A. Finder. *For Some, Online Persona Undermines a Résumé* 2006 [cited 18.08.2008]; Available from: http://www.nytimes.com/2006/06/11/us/11recruit.html?_r=2&oref=slogin&oref=slogin.

[4] D. Rosenblum, *What Anyone Can Know: The Privacy Risks of Social Networking Sites.* IEEE Security and Privacy, 2007. **5**(3): p. 40-49.

[5] CBCNews. *Student recruits unfit for service, say former border guards*. 2007 [cited 18.8.2008]; Available from: http://www.cbc.ca/canada/british-columbia/story/2007/10/01/bc-borderguards.html.

[6] Ofcom, *Social Networking: A quantitative and qualitative research report into attitudes, behaviours and use*. 2008, Office of Communications of United Kingdom.

[7] H. R. Lipford, A. Besmer, and J. Watson, *Understanding Privacy Settings in Facebook with an Audience View*, in *Usability, Psychology, and Security 2008*. 2008: San Francisco, CA. p. 1-8.

[8] A. Felt and D. Evans, *Privacy Protection for Social Networking Platforms* in *W2SP 2008: Web 2.0 Security and Privacy 2008*. 2008: Oakland, California. p 1-8.

[9] E. Aïmeur, G. Brassard, and F. S. M. Onana. *Privacy-preserving demographic filtering*. in *Proceedings of the 2006 ACM symposium on Applied computing*. 2006. Dijon, pp. 872 - 878.

[10] T. Buchanan, C. Paine, A. N. Joinson, and U.-D. Reips, *Development of measures of online privacy concern and protection for use on the Internet.* Journal of the American Society for Information Science and Technology, 2007. **58**(2): p. 157-165.

[11] C. Dwyer, S. R. Hiltz, and K. Passerini. *Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace*. in *Proceedings of the Thirteenth Americas Conference on Information Systems*. 2007. Keystone, Colorado, pp. CD-ROM only.

[12] R. Gross and A. Acquisti. *Information Revelation and Privacy in Online Social Networks*. in *Proceedings of the 2005 Workshop on Privacy in the Electronic Society*. 2005. Alexandria, VA, USA pp. 71 - 80.

[13] M. Mannan and P. C. v. Oorschot. *Privacy-enhanced sharing of personal content on the web*. in *Proceeding of the 17th international conference on World Wide Web*. 2008. Beijing, China ACM, pp. 487-496

[14] M. Hart, R. Johnson, and A. Stent, *More Content - Less Control: Access Control in the Web 2.0*, in *Workshop of Web 2.0 Security & Privacy 2007*. 2007: Oakland, California. p. 1-8.

[15] A. Acquisti and R. Gross. *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*. in *6th Workshop on Privacy Enhancing Technologies*. 2006. Cambridge, U.K, pp. 36-58.

[16] E. Aïmeur, G. Brassard, J. M. Fernandez, F. S. M. Onana, and Z. Rakowski. *Experimental Demonstration of a Hybrid Privacy-Preserving Recommender System*. in *2008 Third International Conference on Availability, Reliability and Security*. 2008. Barcelone, pp. 161-170.

[17] H. Hage, E. Aïmeur, and F. S. M. Onana. *Anonymous Credentials for Privacy-Preserving E-learning*. in *2008 International MCETECH Conference on e-Technologies (mcetech 2008)* 2008. Montreal: MCETECH, pp. 70-80.