

A STUDY ON PRIVACY CONCERNS IN SOCIAL NETWORKING SITES (SNS) AMONG MALAYSIAN STUDENTS

Lau Keng Yew, Ma Meng, Mak Wai Hong, and Nasriah Zakaria

*Universiti Sains Malaysia, Penang, Malaysia,
kengyew_88@yahoo.com, esionma@gmail.com, waihongmak@hotmail.com, nasriah@cs.usm.my*

ABSTRACT. The rise in popularity of social networking sites (SNS) has led to various social and ethical issues such as privacy. The freedom to share and post information, pictures and to network with each other have raised privacy concerns among SNS members. We carried out a survey of 100 students at one of Malaysian universities to analyze their behavior on the SNSs in terms of awareness of privacy protection and what actions they have been taken. The survey results show that most of the students are aware of the customizable privacy settings but less than half of them change or modify them. This survey is important for understanding the user's approach to privacy protection, which in turn is important for our proposed privacy protection systems in future research.

Keywords: Social Networking Sites (SNS), Privacy, Disclosure

INTRODUCTION

Social networking sites (SNS) arise as a new type of communication tool, open to all categories of users whether young or old. SNS begin replacing face to face interaction as a primary communication medium due to the fact that the internet can be accessible everywhere nowadays. A user can have a chat session, sharing photos and viewing her friends' status anytime by just sitting in front of computer without going out of her home. Facebook for example has millions of members signing in every day as it is very convenient. It also can be used to reconnect long lost friends as well as to socialize with others. However, these types of technology have brought in various social issues and privacy concerns. Many users, especially the young generation, do not think twice about providing as much information as possible on their profile without realizing the privacy risks they will be facing. They are willing to disclose their personal data in order to get more friends and network with strangers, without having thought of the consequences of their action. These users ignore the fact that the advanced technology of Internet search engines like Google makes it possible for strangers to find their personal information and details in just few seconds. Employers have searched to find more information about their future employees or to monitor their current workers. The SNS itself does not warn the user of the dangers of disclosing their information to everyone, because the purpose of social networking is to share and communicate with others. Facebook had an "opt-in" policy (Stana & Burton, 2002) for their privacy setting, which means that a user's information can be searched and seen by everyone by default. This policy will catch out many new members and first-time users who are not aware of it or what it means to have their personal data leaked and disclosed to strangers. It will result in various privacy threats (Facebook website) and crimes like identity theft, harassment, spamming and phishing. Another concern is that most of the third party applications or also known as "apps" mentioned by Krishnamurthy and Wills (2008) in Facebook collect users' personal information

and contacts without permission and use or sell the data for advertising purposes. This shows that there will be many more threats and risks the user will face if they do not take active steps to protect their privacy, rather than relying on the social networking sites policies.

The objective of this paper is to explore the online behavior relating to privacy of students in Malaysia and to explore how users manage their existing privacy settings in SNS.

RELATED WORK

Personal information can be categorized into public and private. According to Petronio's Communication Privacy Management theory (2007), users should have clear ownership and control of their information in SNS. This means that all their information should be customized as either public or private through the configuration of privacy settings. Altman (1975), one of the authoritative scholars in privacy research stated that every user has a different level of privacy needs and control over who can access their data. There are many factors that influence user privacy including age, sex, culture and family background. One of the main reasons that users do not protect their privacy is the design of the privacy settings interface itself (Lampe et al., 2006). For an example, configuring privacy settings in most social networking sites are difficult because it requires the understanding of the many settings that can be modified and numerous ways of controlling those entire users' information to prevent other gaining access to their information. For an example, in one of the well known SNS sites, choosing the opt in privacy policy means that the default privacy settings for all users are to make their information public and accessible to everyone (Stana & Burton, 2002). Barnes (2006) stated that users more easily provide and reveal personal information on SNS than on other communication tools such as the telephone or face to face conversation. The reason that users share their information willingly is to gain more friends and contacts in SNS which has become a popular venue as they feel that they can express themselves more by socializing virtually than in real time. Hence, Krishnamurthy and Wills (2008) suggested that users' information in SNS should be divided into categories that can range from most confidential to least private. Information that is considered sensitive, such as home address, phone number and personal photos need to be made private to avoid the consequences of privacy invasion.

Another reason for joining SNS is peer pressure (Acquisti & Gross, 2006). Acquisti and Gross (2006) discovered that most users tend to follow their friends' lead in the amount of information disclosed and shared. This finding led to a research work by Bonneau and team (Bonneau et al., 2008) where they developed a tool known as a *Privacy Suite*, which enables a users to adapt their friends' privacy settings to their own. Although it appears a simple solution that saves time, it is not a long term solution. This scenario may actually cause more privacy issues and concerns since one user's preference may not suitable with others and some sensitive information may be leaked out.

Similar surveys have been done by researchers on privacy concerns and disclosure habits of university students. Acquisti and Gross (2005) found that only minimal number of students changed their default privacy settings in a SNS leaving their profile information visible and accessible to everyone. On the other hand, Govani and Pashley (2009) found the students were aware of the privacy risks but choose not to modify their privacy settings in order to get more friends and contacts. In conclusion, there are many concerns on the level of user awareness on privacy and how the privacy settings in SNS are set. Most of the empirical work is done in the Western countries while our paper attempts to explore the privacy awareness among Asian (particularly Malaysia) users.

METHOD

A survey was given to 100 students at one local university in Malaysia. We chose a university setting with the assumption university students are one of the most active SNS users. The objective of the survey was to collect data on students' information disclosure

behaviors and how they manage their privacy settings in SNS. We chose a well known SNS as a reference in this study. We did not face any problem finding participants as most of the students own an account in this well-known SNS. A follow-up interviews were also conducted with a few students to gain a more in-depth understanding of their perception of privacy levels and precautions and the difficulties encountered when configuring privacy settings. Similarities among students according to categories of gender, culture and age are identified. We chose the method of survey for the study because it allowed us to get great deal of valuable data in a short time, as well as we hoped increasing the awareness of students about protecting their privacy. The survey contained thirteen questions in formats including multiple choices; fill in the blanks, and short answer/personal opinion: these mainly focused on privacy and disclosure management.

RESULTS AND DISCUSSION

Analysis of the 100 completed survey forms from students gave some perspectives of Malaysian students' view about their privacy concerns on SNS. In the following sections, we discuss the views of the students about their privacy concerns based the majority answers to the survey paper.

Out of the 100 respondents, 79 of them are Chinese students followed by 15 Malay(native) students and 6 Indian students. The age of the participants ranged from 20 to 29 years old-some are graduate students, with the majority (78%) of the participants 22-23 years old. In terms of gender, 51% of participants were male and 49% female. Therefore, we are able to get a representative data in terms of gender.

Our questions focused on a particular SNS, a well known among the students. Question 1 asks the student's reason for joining the SNS. Based on the feedback from the students, 13 students joined to find a friend they knew, 22 students due to peer pressure, 59 students in order to socialize and network with friends, and 6 for "others reason" for joining SNS, including for game and for fun only. For the majority of the students, it is clear the reason of joining the particular SNS is mainly for socialization. They are keen to communicate and socialize in this online community; they are willing to exchange a lot of information during their communication. Hence, this question shows the users ignore the confidentiality of their information and protection of privacy for the sake of socialization and this is closely related to our survey regarding the privacy concern of the students. This gives us strong motivation for discussion of and research into the topic of privacy since information is very vulnerable nowadays due to Internet technology.

The subsequent questions ask about the student's privacy concerns before they began using and now when they are actively using SNS. The second question asks the students whether they read through the privacy terms when (or before) they signed up for their SNS account. The results are skewed where the majority of the participants, 88% responded that they did not read before or during signing up the SNS account. We found that only 12% of the participants answered that they read through the privacy conditions or terms. The responses to this survey question indicate that the participants are less concerned about the privacy policies provided by the SNS. This kind of attitude may eventually cause the users to violate the privacy rules without realizing that they are doing so, because they are not aware of the activities/information that are restricted in the SNS.

Question 3 and 4 asked for the participant's opinions about what sort of information they provided when they signed up for their SNS account and which kinds of information that they considered to be private and should not be disclosed to the public without the permission of the user himself. The types of information that survey participants considered private are shown in Figure 1. The information most frequently cited as private is phone number and home address; because public knowledge of this information could result in unwanted disturbance from strangers or people that the user does not wish to see.

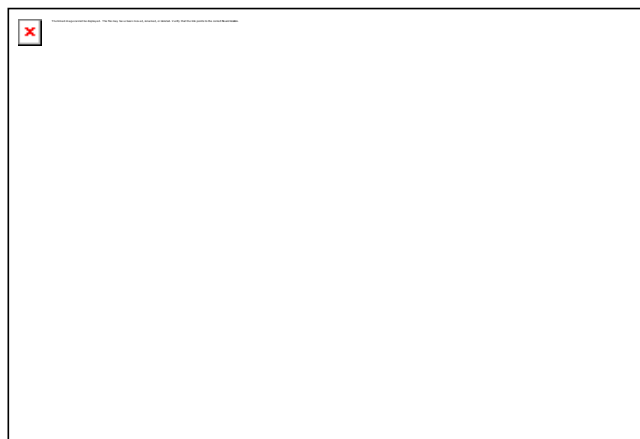


Figure 32: The Privacy level of users' information

Question 5 asks how often the users log in to their accounts. Most of the users (68%) log in daily, 22% log in several times per day, and 11% log in weekly or monthly. This shows that they are using the SNS to communicate at least once per day. This enables us to see how often users have the chance to be updated with new privacy setting of the SNS.

Question 6 asks whether the users are aware they can change their privacy settings in the SNS. The results show that almost all are aware, with 84% of participants' aware and 16% not aware. Question 7 explored how the users manage the privacy setting in SNS accounts. The distribution of responses to question 7 is shown in Figure 2. The results show that 45% of the participants manage their privacy by only adding the friends they know, 36% of the participants manage by customizing their privacy settings, 22% provide limited information in their account, and 4% said they did not really care about it. (Percentages sum to more than 100% because users could select more than one option) Responses to question 8 show that 95% of the participants think that privacy management is important for their SNS accounts. By combining the responses of questions 6, 7 and 8, we can see that most of the students do realize that they can control and manage their privacy settings in SNS, they realize the importance of privacy management in SNS, and they have or develop their own ways to manage and control their privacy in SNS. Therefore, we can conclude that the majority of the users do have high concerns about the privacy protection of their SNS account information.

Based on the responses of the question 9, we found that 89% of the participants do not trust the privacy protections that are provided by SNS and think that information posed to SNS is not safe and private. This strongly indicates that there is a need for higher level privacy protection tools to be built for and provided to SNS's users. Since a majority of the users manage their privacy by adding only friends they know, question 10 delves further into the user's selection of friends by asking whether they check the information of a friend that has been approved and accepted via a friend request, to confirm their real identity. 78% of the participants do check and confirm the identity of friend requests, but 22% do not. It is important for users to confirm the real identity of the friend that they have added, because some individuals may use a nick name for their profile which is unknown in order to protect their privacy.

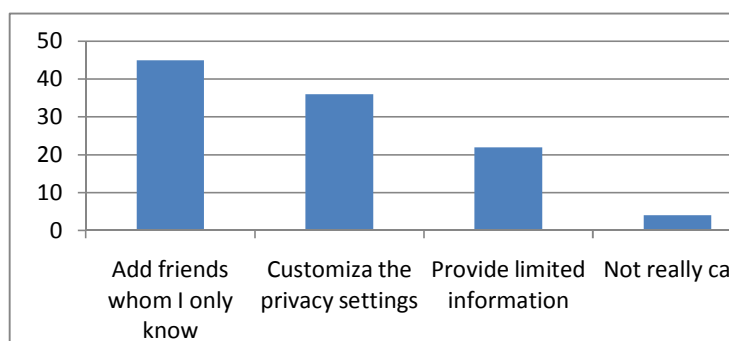


Figure 33: Method for protecting privacy

Question 11 is related to question 5; it further queries participants on how often they update their profile, especially the privacy part. This further tells us how often they keep up to date with new privacy configuration in their SNS accounts. 85% of the participants said they update their profile seldom or annually, 10% said monthly or weekly, and 5% said they had no fixed time for update. This shows that users seldom update their profile and therefore also their privacy settings. This is not a good sign for privacy management, users need to evaluate and update their privacy settings regularly instead of annually or never. This issue indirectly shows that users need a tool that will regularly alert them and help them to evaluate their privacy settings and help them with privacy management and updating whenever there is a need.

Question 12 asked participants whether they have ever misused information from another person's profile. 95% of participants answered no, the 5% that had misused someone else's profile said their purpose was not to do something harmful but just play a joke on their friends. However, misuse of another's profile is still an action of information violation and identity theft, and should be considered as serious as cyber crime. Therefore, the SNS should enhance their privacy protection level, so that, users' information can be more secure. Users also should change their attitude and know that identity theft is an unethical action. Users should cooperate with their SNS in privacy protection and management in order to create a more secure communication environment for users themselves.

Nowadays, SNS are fast becoming more and more useful communication tool; so, more and more privacy management and protection should be provided for secure communications. However, do users think that SNS will replace verbal communication in the future? Survey question 13 shows that 31% of the participants believe not. On the other hand, 69% do believe that SNS will replace verbal communication in the future, and the majority provided some arguments for this view, including the fact that that communication via the Internet can save time and reduce working stress.

CONCLUSION AND FUTURE WORK

In conclusion, user' concern about privacy issues on SNS is high. Survey results show that the majority of users are aware of the existence of the privacy settings provided in their SNS, but most of them are ignorant about specific policies and options; some users do not even care about privacy in their SNS. The survey also shows that users believe that part of the responsibility for privacy should fall to the SNS providers because they provide security levels and options for information protection that are not at the expected level and should be further enhanced. In reality, of course, the responsibility for privacy protection should lie with both SNS and SNS users, both should work together and give support and co-operation to each other in order to enhance the privacy protection of SNS, reduce cyber crime and enable a more secure communication era for the generation in future.

This survey can contribute to future analysis of the difference between Asian and Western citizens' privacy concerns to look more deeply into culture as the main factor that affects a person's privacy view as a whole. This survey also can contribute to the development of a privacy management system because it can help developers understand what users are concerned about in relation to privacy settings, and what users expect from SNS in privacy management. This will indirectly assist in the creation of a privacy management system that will fulfill all user expectation and protect users more securely in future.

ACKNOWLEDGMENTS

We would like to thank our coordinator who provides guidance for us to conduct this research paper. We also appreciate the help of the reviewers of participants in the survey, and other individuals who indirectly made a contribution to this research.

REFERENCES

- Acquisti A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on Facebook. In: Danezis, G., Golle, P. (Eds.), *PET 2006. LNCS*, Vol. 4258, (pp. 36–58). Springer, Heidelberg.
- Acquisti, A., & Gross, R. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook Case), *ACM Workshop on Privacy in the Electronic Society (WPES)*, (pp. 1-11).
- Krishnamurthy, B., & Wills, C. E. (2008). Characterizing privacy in online social networks. *Proceedings of the First Workshop on Online Social Networks. WOSP '08. ACM*, New York, NY, (pp. 37-42).
- Altman, I. (1975). *The Environment and Social Behavior*. Monterey, California: Brooks/Cole.
- Barnes, S. B. (2006, September 4). A privacy paradox: Social networking in the United States. Retrieved from <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312>
- Bonneau, J., Anderson, J., & Church, L. (2009). Privacy Suites: Shared Privacy for Social Networks. *ACM International Conference Proceedings of the 5th Symposium on Usable Privacy and Security*, (pp.1-2).
- Facebook website. Retrieved from <http://www.facebook.com/>
- Lampe, C., Ellison, N., & Steinfield, C. (2006). A face(book) in the crowd: social searching vs. social browsing. *Proceedings of the Conference on Computer Supported Cooperative Work*, Banff, Alberta, Canada, (pp.167-170).
- Petronio, S. (2007). Translational Research Endeavors and the Practices of Communication Privacy Management. *Journal of Applied Communication Research*, 35(3), 218-222.
- Govani, T., & Pashley, H. (2007). Student Awareness of the Implications when Using Facebook. (pp. 4-17). Retrieved from <http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf>
- Stana, R. M., & Burton, D. R. (2002). Identity Theft: Prevalence and Cost Appear to be Growing. Tech. Rep. GAO-02-363, U.S. General Accounting Office, Washington, DC.