User Oriented Privacy Model for Social Networks

Nader Yahya Alkeinay*, Norita Md. Norwawi

*USIM, BBN, Nilai, 71800, Malaysia

Abstract

Social Networking Sites (SNSs) have become a global experience, with communities such as Facebook, MySpace and Friendster which they are reporting user figures in the hundreds of millions. People, have been invited into or chosen to join these communities are able to publish multimedia content about themselves, their interests and concerns. With intensive information been shared, privacy concern are rising up because Social networks privacy is different from the classic privacy setting that cause a lot of problems such as exposing sensitive information. On the other hand privacy model should be designed to facilitate user’s requirements, which mean that users are, supposed to set up their own privacy setting. Since it’s still not well defined and need to be improved and studied further. However, to solve this is by providing a more private platform with the ability for users to set their own privacy settings. The privacy model can be so general to more complicated, but all of them are still not clear for users to be aware off. The new model we are proposing will solve the privacy issues since it’s done by users and monitored by developers. This research will point out some problems, and how to solve these problems by proposing a new user oriented privacy model for social networks.

1. Introduction

Online social networks are websites that let users to build connections and relationships to other Internet users. Social networks store information remotely, rather than on a user’s personal computer.

* Corresponding author.
E-mail address: nyma@outlook.com.
Social networking can be used to keep in touch with friends, make new contacts and find people with similar interests and ideas. These days we can see that almost if not everyone are using the internet, so every one of us are using one or more social network, some of us they use YouTube for videos and others they use LinkedIn, Facebook and MySpace for social interaction. However, the many online communities can be broken down into major categories such as informational, professional, educational, hobbies, academic, and news related. Within each of these major categories, there are thousands of communities filled with active members who dedicate a fair share of their day to participate in those social networks. On the other hand data collected by social networks are an important source for social and marketing analysis, which may provide useful information on the evolution of a social community, collaborative problem solving, information distribution, and so on.

2. Literature Review

In this research we will emphasize in three social networks which are (Facebook, MySpace and Friendster) we choose these three because it’s well known and they have a lot of users together with some issues in the way they handle the user’s privacy. Privacy is playing a major role in social networks since its more about information so the privacy of what information we share is very important to protect us and our rights. However, every social network are doing the best in protecting information but still there has been a lot of cases because of the misunderstand of the privacy, so privacy issues here are in the top of problems facing any social network.

2.1 Information sharing theory

Natural information sharing behaviours also grow during the process of growing up, as the character gets modified by environment and learning. People have social interactions and their behaviours may change accordingly. Social models and culture also play a role to influence the behaviour. In one study, 3-year-old children shared more often if the recipients had shared with them previously (Olson & Spelke, 2008). So children begin to learn from whom to be nice to according to their own experiences with them. This has its evolutionary cause because we can also find information sharing behaviours in animals. For example, when bees find good sources of honey, they would “dance” in a firm style to share the information and the route to the honey sources to their peers so that others can also go there (Seeley 1995). Ants also have an instinct to communicate with their peers when they find food sources (Adler & Gordon, 1992). These sharing behaviours are innate behaviours in nature. As people join social networking sites, they begin on creating a profile, then make relations to existing friends as well as those they meet through the site. A profile is an inventory of information identifying. It can include your real name, or a false name. It also can include photographs, birthday, hometown, religion, background, and personal interest may be correct information or false. Members join others by sending a “friend” message, which must be accepted by the other party in order to establish a link. “Friending” another member gives them access to your profile, adds them to your social network, and vice versa. Members use these sites for a number of purposes. The root motivation is communication and maintaining relationships. Popular activities include updating others on activities and whereabouts, 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.

2.1 Privacy

Privacy is the right or opportunity to decide who has access to your personal information and how that information should be used. The issue of privacy within social networking sites is often not expected or
is undefined. On the other hand privacy issues in social network is not the same in other websites because of the information that been shared among users. For any user of the Facebook, other users can be defined or groups into four different groups: Friends, Friends of friends, Non-friend users at the same institution, and Non-friend users at a different institution. According to (W. Mackay, 1991) by default, everybody on the Facebook appears in searches of everyone else, independent of the searchers institutional membership. In search results the user’s full names for examples first names are possible appear along with the profile image, the academic organization that the user is attending and the user’s status there and so on.

2.3 API Implication

API which stands for Application Programming Interface, means that any application or developer can develop and applications and run it directly in few minutes in Facebook or other social network, the applications can be anything and it’s entitled to take all your information and use it as they want. Adrienne Felt, at Berkeley, made small headlines in 2007 when she exposed a potentially devastating hole in the framework of Facebook's third-party application programming interface (API) which allows for easy theft of private information. Felt and her co-researchers found that third-party platform applications for Facebook gave developers access to far more information (addresses, pictures, interests, etc.) than needed to run the app.

3. Methodology

This study applied quantitative method in order to analyse data and get important information such as: demographic information of the respondents. In this case a questionnaire method will be used and distributed to over more than 200 social networks users the population will be determined by the snowball rolling since snowball sampling is a non–probability sampling technique. Snowball sampling and respondent-driven sampling also allows researchers to make estimates about the social network connecting the hidden population to ask them on the privacy of the existing social networks.

4. Finding and Analysis

4.1 Demographic and Social Network Information

This study aims at finding the privacy and security in online social network sites perception among SN users. A sample of 200 students was selected randomly from different part of the world. A net of 161 questionnaires were filled correctly and returned. Nearly 57% of the respondents were males, while nearly 43% of them were females. On the other hand, approximately 83% of respondents were in the age group 18-29 years old. However, the number of respondents in the age groups “between 30-49 almost got 15% where other groups 50 and above is almost zero. Educational level played a very high impact since 64% are bachelor degree and graduate degrees are 23%. The years of using Internet reflect on the familiarity of social network because from those are using the internet for more than 10 years are 49% and if we link the usage with familiarity of SN it shows 40 % for moderately familiar and 44% for very familiar. On the other hand 98% of this survey population is using Facebook and 57 % using IslamTag and 52% twitter so this is an advantage for us to study Facebook privacy model.
4.2 Privacy

Table 1 shows that when asking about privacy and how well they are aware of privacy and terms of conditions 44% are moderately familiar with the features and updates in SN privacy which was proven that they are familiar with the privacy when 80% restrict access some for certain part in their profile. But when it comes to changing privacy 41% change their privacy setting occasionally which means only if anything happened and 40% rarely change their privacy setting and the same goes for security and account setting.

| Frequency                  | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------------------|-----------|---------|---------------|--------------------|
| Extremely familiar         | 7         | 4.3     | 4.3           | 4.3                |
| Moderately familiar        | 71        | 11.1    | 11.1          | 18.1               |
| Not at all familiar        | 2         | 1.2     | 1.2           | 19.7               |
| Slightly familiar          | 40        | 24.8    | 24.8          | 74.8               |
| Very familiar              | 41        | 25.5    | 25.5          | 100.0              |
| Total                      | 161       | 100.00  | 100.00        |                    |

4.3 Information Sharing

According to figure 1, sharing is humans nature and from this survey we found out that 61% said that they sometimes share accurate information and their photos to the public and without any kind of restriction and only 16% said that they never share accurate information about themselves on the other hand 23% they do sharing all the time. However, the awareness level of sharing their location using geo on their phone or laptop is very high because according to table 2 shows the awareness of location privacy and its issues on SN. Initially, about 17% of respondents felt that they need to share their location and they don’t care about their privacy of personal information is not protected at all, whereas 30% of respondent share their location if they uses mobile phone and 53% of respondent felt like they need some privacy by not sharing their location, which means the privacy of their personal information such as location is slightly protected.

| Frequency                  | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------------------|-----------|---------|---------------|--------------------|
| A) Only on my phone        | 28        | 29.8    | 29.8          | 29.8               |
| B) Yes in all my devices   | 27        | 16.8    | 16.8          | 46.6               |
| C) No I don’t want anyone to know where | 85        | 53.4    | 53.4          | 100.0              |
| Total                      | 161       | 100.00  | 100.00        |                    |
4.4 Information Sharing

When it comes to security and protecting our data we tried our best level to secure or data specially when dealing with money but when it comes to information we forget that it has a value also and from the graph it shows that 68% don’t care about protecting and using a complex password where only 32% they use complex which is a mix of letters, numbers and symbols. On the same issue but using mobile phone only 52% lock their phones with passcode and 48% leave their info wide open.

All of that careless but still they are aware of every issues in social network – 60% are aware of employee checks on social network for their background but still they expose themselves . Though we asked them that if social networks didn’t respect your privacy and your security will you leave the site or reduce the amount of information shared and the answer was 61% to reduce the among of information been shared.

5. Conclusion and Recommendation

The importance of online social networks sites to human social development cannot be over reduced but it needs away to fix it. On the other hand privacy and security of a social network is not the same as any web2.0 because in social networks you are dealing with data integration and online social networks sites allowed people to interact to each other freely, conduct businesses and above all serve as a media for all. Therefore, this study found that social network developers need to understand the concept of privacy and to create a model for privacy to suit the needs of users and to protect their data. Because the majority are not aware of the issues of privacy and security threat that were usually vulnerable to in online social networks environment. In addition to that they continue to use social networking sites nevertheless their understanding of the sites privacy and security policy, and this usually lead to the conceding their personal identification secrecy. Therefore, this study suggested building a model that can protect user’s information as well as increase the trust in social networks developers.
Acknowledgements

My heartfelt appreciation goes to Research committee who provided helpful comments and suggestions. Finally, I would like to express my gratitude to USIM for their financial support.

References

Gail-Joon Ahn, Mohamed Shehab, Anna Squicciarini. 2011. "Security and Privacy in Social Networks". *IEEE Internet Computing*. vol. 15, no. 3, pp. 10-12, , doi:10.1109/MIC.2011.66

Kristina R. Olson, Elizabeth S. Spelke. 2007. “Foundations of cooperation in young children” Psychology Department. Harvard University. USA.

Thomas D Seeley. 1997. “Honey Bee Clonies Are Group-Level Adaptive Units”. cornell University. N.a.. 2011. “Implementation of the Safer Social Networking Principles for the EU”. http://ec.europa.eu/information_society/activities/social_networking.eu_action/implementation_princip/index_en.htm . Europe’s information society.

W. Mackay. 1991. “Triggers and barriers to customizing software.” In Proceedings of CHI’91, 153–160. ACM Press.

Balachander Krishnamurthy, Craig E. Wills, 2010. “Privacy Leakage in Mobile Online Social Networks”. AT&T Labs. Worcester Polytechnic Institute. USA

N.a.. 2011. “Hiring Managers Have Used Internet Search Engines to Screen Job Candidates” http://www.creativepro.com/article/one-in-four-hiring-managers-have-used-internet-search-engines-to-screen-job-candidates. CareerBuilder.com

Emily Maitlis. 2011. BBC Documentary “Inside Facebook”. http://www.youtube.com/watch?v=tlQbtNn3-vI

Lipford, H., Besmer, A., Watson, J. 2008. “Understanding Privacy Settings on Facebook with an Audience View”.

P. G. Lange. 2007. “Publicly Private and Privately Public” Social Networking on YouTube. Journal of Computer-Mediated Communication, 13: article 18.

Churchill, E. F. and Halverson, C. A. October 2005. “Social Networks and Social Networking”. *IEEE Internet Computing*, 9, 5, "14-19.

Johnson, G. J. and Ambrose, P. J. 2006. “Neo-tribes: the power and potential of online communities in health care”. *Communication ACM*, 49, 1, 107-113.

Cummings, J. N., Butler, B. and Kraut, R. .July 2002. “The Quality of Online Social Relationships”. *Communications of the ACM*, 45, 7, 103-108.

Cross, R. and Parker, A. 2004. “The hidden power of social networks”. Boston: Harvard Business School Press.
Boyd, D. M. and Ellison, N. B. 2007. “Social network sites: Definition, history, and scholarship”. *Journal of Computer-Mediated Communication*, 13, 1, Article 11.

Tim Wafa. June 2009. “Global Internet Privacy Rights” – A Pragmatic Approach. University of San Francisco Intellectual Property Law Bulletin.

Coppola, N., S. R. Hiltz, and N. Rotter. 2004. “Building Trust in Virtual Teams,” *IEEE Transactions on Professional Communication* (47) 2, pp. 95-104.

Frank, O. 1979. "Estimation of population totals by use of snowball samples". *Perspectives on Social Network Research*. 319-47