Students' Perception of Privacy Risks in Using Social Networking Sites for Learning: A Study of Uganda Christian University

Francis Otto(✉), Nurul Amin Badrul, Shirley Williams, and Karsten Øster Lundqvist

School of Systems Engineering, University of Reading, Reading, UK
{f.otto,n.a.badrul}@pgr.reading.ac.uk,
{shirley.williams,k.o.lundqvist}@reading.ac.uk

Abstract. Although social networking sites (SNSs) present a great deal of opportunities to support learning, the privacy risk is perceived by learners as a friction point that affects their full use for learning. Privacy risks in SNSs can be divided into risks that are posed by the SNS provider itself and risks that result from user's social interactions. Using an online survey questionnaire, this study explored the students' perception of the benefits in using social networking sites for learning purposes and their perceived privacy risks. A sample of 214 students from Uganda Christian University in Africa was studied. The results show that although 88 % of participants indicated the usefulness of SNSs for learning, they are also aware of the risks associated with these sites. Most of the participants are concerned with privacy risks such as identity theft, cyber bullying, and impersonation that might influence their online learning participation in SNSs.

Keywords: Social networking sites · Online social network · Privacy risks · Learning · Students

1 Introduction

One of the contentious topics that emerge when communication is mediated by a social networking site (SNS) is the privacy issue [1]. Although SNSs present a great deal of opportunities to support learning, the privacy risk is perceived by learners as a friction point that affects its full use for learning. Users of these sites often establish hundreds to even thousands of online social networks (OSN) with other users whom they interact and collaborate in their daily life.

SNSs are "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" [2]. They facilitate sharing, interaction and collaboration among users [3–5]. Although they are commercial products initially designed for the social interaction purpose [6], these sites have a powerful influence on all aspects of life [7] and provide great potentials for transforming the learning process [4, 5].

G. Vincenti et al. (Eds.): eLEOT 2015, LNICST 160, pp. 182–190, 2016.
DOI: 10.1007/978-3-319-28883-3_23

Since the basic principle of SNS is information sharing, SNS providers encourage their users to actively participate and interact in their network. Thus, the higher the number of (particularly active) users, the higher value a particular SNS holds. This is the reason why SNS providers focus on the 'quality' of the content in ensuring better connectivity to their users [8]. In order to achieve this, one approach is by implementing 'real name policy' by requiring users to provide their real name and information [9] when signing up.

However providing real name and personal information may invite privacy risks to users. Users who participate in SNSs voluntarily share their personal information with their 'friends' online. By disclosing their personal information, users are vulnerable to privacy risks in SNSs [10]. With the growing popularity and massive amount of personal information (the largest database), SNSs are vulnerable to cyber-attacks [11].

Whereas users do perceive the use of SNS for learning, the imminent privacy concern may affect their full interaction and collaboration whilst they are online. This study explored the perception of undergraduate students of Uganda Christian University on the use of SNSs for learning purpose and their perceived privacy risks.

2 Background

Social networking has occurred almost as long as societies themselves have existed but the potential of the online (social networking) tools have made it a more popular concept especially among the younger Internet users, who are able to create and disseminate contents to their friends [12]. The concept of social networking refers to the practice of expanding the number of one's social network by making connections through other individuals. By so doing, individuals build online social networks (OSN) or social relations among people who share interests, activities, backgrounds or real-life connections.

Use of SNSs has become commonplace within higher education as they facilitate active participation, connectivity, collaboration and sharing of knowledge and ideas among learners [4]. Since they are a read-write form of Web [13, 14], they are very useful for learning purposes. However the privacy risks associated with the use of these sites may affect their full utilization for learning.

One of the privacy concerns involving the use of SNSs is the users' personal information that is being shared online. While SNSs allow users to restrict access to their personal data, there is currently no mechanism to enforce privacy concerns over materials posted by them [15] or by other users about them. As information that a user posts may be shared by others, privacy of this information goes beyond the discretion the user. What Facebook, Google+, LinkedIn and other SNSs do with our data, and what they enable others to do, too is a big concern for users.

Therefore users' privacy concerns might reduce their full participation in online learning because users are considering the trade-offs between the perceived benefit and risk of their participation. This behavior which is typically known as privacy calculus theory suggest that users intention to disclose information will depend on privacy concern and expected benefit [16].

In general privacy risks in SNSs can be categorised into two dimensions that is, a vertical risk and a horizontal risk [17]. The, vertical risks are the risks posed by the SNS provider itself in using personal data, aggregating and collecting information while the horizontal risks represent social interactions among the users where they share their information, thoughts and activities.

2.1 Vertical Privacy Risks

The literature suggests that SNS provider's privacy policy is one of user's privacy concerns [17–20]. In a survey of 45 SNSs, research in [18] discovered that although most SNSs have a privacy policy, many are considered substandard, and some have no privacy policy at all. The researchers discovered in their study that two sites integrate privacy policy with *Terms of Use*, one site has questionable privacy policy, and generally all sites provide lengthy privacy policies which discourage users from reading fully.

Additionally, SNS providers are authorised to amend the content of agreement without the requirement to refer to the user. Further to their findings, it was discovered that the best SNSs will act is providing a minimum notice period before any changes takes effect [18]. However this clause only appears in 11 % of the total SNSs surveyed. The default privacy settings in Facebook (at the time of the research), for example aggravate to the problem of privacy where it is at the lowest privacy level and requires user to be proactive if they want to protect their privacy [17].

Furthermore, researchers also reported that SNSs specifically Facebook's privacy practices is poor, insufficient and misleading [19]. One example of Facebook's confusing privacy policies was the changing of user's privacy configuration four times in four years between 2006 to 2010 [20].

In general, SNS providers have the advantages of collecting a great deal of information about their users and further use this for offering personalisation services and sharing with third parties. They are involved in selling these information to third parties [11]. Since SNSs offer their services for free, the main and only source of income is targeted advertising, the selling of personal information to third parties assists in their sustainability [11].

2.2 Horizontal Privacy Risks

On the other hand, user's willingness to disclose too much information is another factor that affects user's privacy. Although users are concerned about what and to whom they share, most of them have limited understanding of how to manage their profile privacy settings. This has led to user's personal information being highly visible to unintended audience. The abundance of information has attracted various parties who might misuse the viewable contents. SNSs have become an important and a convenient source of targets for their malicious activities [21]. While sharing (sensitive) information with online friends can facilitate relationship development, the behaviour of online friends can reveal a user's personal information [22].

SNSs attract many horizontal privacy risks such as identity theft attacks, since this kind of attack is relatively cheap to implement and difficult to prosecute [23]. With the rapid development and advancement of online technologies, the attackers simply collects available personal information from SNSs and uses that personal information in an unauthorized manner with the intention to commit fraud or other crimes [11]. Another example of horizontal privacy risk is cyber bullying, which refers to harassment that makes use of technologies such as email, text, mobile phones, and websites [24]. There is also another risk known as social surveillance. Social surveillance is an act of observing SNS users in order to gain awareness of their offline and online behaviour. This may be done by the government or individual SNS users [26]. Besides building relationship and keeping in touch with friends, SNSs are also being used for social surveillance purpose [25]. Government and individuals are able to monitor users' behaviour and get updated on their activities. This high-degree of surveillance can cause privacy concerns to users [26].

3 Methodology

3.1 Research Questions

The main aim of this study was to explore students' perception of the benefit in using SNSs for learning purposes and their perceived privacy risks. The following research questions were set to guide this study:

i. What do students think about the usefulness of social networking sites in supporting their learning activities?
ii. What are the negative effects of using social networking sites for learning purposes?

In answering these research questions, this work explored the various types of risks associated with social networking sites mentioned in literature whilst matching them with what were perceived by the students who participated in this study. The result of which will illustrate the emerging gap and effects of these risks on the participation of users online.

3.2 Selection of Participants

In this study, a convenience sample of 214 participants was drawn from Uganda Christian University, where the study was based. Uganda Christian University has over 11,000 students offering a wide range of programmes at its five campuses throughout Uganda. However, the study was based at the main campus with some 6,000 students within seven units (one school and six faculties). The participants in this study were drawn from the six faculties using the class schedules and year of study. Before recruitment, they were briefed about the study by the research team. Participation was completely voluntary but informed consent was sought prior to administering the survey. A fairly balanced gender participation was realized; 124 (57.9 %) were male, 88 (41.1 %) were female, while 2 (0.9 %) preferred not to specify their gender. 199 (93 %) of the participants were of age group 18–25 years, 11 (5.1 %) were between 26 and 30 years old and 4 (1.8 %) were above 30 years old. The majority of participants were undergraduate students taking Bachelor's Degree (82.7 %), Diploma (14.5 %), and Certificate (0.9 %).

3.3 Data Collection and Analysis

This study was part of the doctoral research which employed a mixed method approach involving survey questionnaires, interviews, focus groups, and observation. However, the data reported here was collected in the first round of data collection using online survey questionnaire. The survey was designed using Google docs and participants accessed the online survey through a link that was provided to them by the research team. Questions of quantitative and qualitative nature were asked. A computer software tool, NVivo version 10 was used to analyze the qualitative data.

4 Findings

It was evident from the data obtained that social networking sites (SNSs) and other online social network (OSN) tools have become commonplace among the students. 195 (91.1 %) of the participants reported to have at least one social network profile and only 19 (8.9 %) did not have any social network profile. This result indicate higher usage than what was reported in a study by Pew Research Center in 2009 about the social network sites usage by young adult in the US, indicating that some 72 % of the users were in the age group 18–29 years had social networking profiles [27].

4.1 Benefits of SNSs

On the question of what they think about the usefulness of social networking sites in supporting their learning activities, participants overwhelmingly responded positively: 124 (57.9 %) indicated that SNSs are very useful, 65 (30.4 %) responded that SNSs are useful, and only 1 (0.5 %) indicated that SNSs are not useful. Whilst 3 (1.4 %) were not sure about the usefulness, 21 (9.8 %) didn't express any feeling about the usefulness of SNS.

4.2 Privacy Risks Perception by Students

Whereas the majority (88.3 %) of participants indicated that SNSs are useful in supporting their learning, they also identified several privacy risks that limit their full participation whilst using these tools. In fact, all of the risks, highlighted by participants, fall under horizontal privacy risks category. No mention was made of the vertical privacy risks.

Generally, most of the horizontal risks are more easily noticeable hence, they are more aware of them. Most of the responses reflected personal experience meaning that one has had an encounter with the incidence resulting from these risks. As a result, many participants reported to have had negative motivation to use SNSs for learning purposes.

4.3 Types of Privacy Risks

In responding to the question of what risks on the OSN that negatively impacts their learning, participants reported several risks, mainly from social aspect of their lives which had impact on the way they use these tools for learning. The types of privacy risks perceived by the participants fall under horizontal privacy risks which have been explained below:

Identity Theft: Many respondents indicated that the greatest privacy risk to them is theft of their identity by unscrupulous attackers. When a malicious person fraudulently gains knowledge of sensitive personal information such as social security number, name, address, phone number, cell number or even banking and credit card information, he/she could do a number of things with that including committing fraud using a person's identity. The respondents felt that the SNSs are insecure and therefore attractive to hackers and 'con men' who may get access to their profiles and personal information.

Impersonation: The respondents expressed concern about the exposure of personal information specifically on false identity or impersonation "it can lead to impersonation in order to attain the information by false pretence". They felt nearly all SNSs that they use do not possess a feasible measure to prevent exposure or abuse of other users' personal information which can go viral over the OSN. Currently, privacy in SNSs cannot be entirely maintained and established by individuals, as it is not wholly dependent on individual choices or control over data. According to [28], providing private information protection within a networked context is determined through a combination of audience, technical mechanisms, and social norms. Because contexts shift and overlap over time, protecting personal information is a continuous and active process.

Cyber Bullying: Some of the respondents expressed the risk of disturbance from colleagues or strangers. Cyber bullying is harassment which makes use of technologies such as email, text, mobile phones, and websites [24]. One of the forms of cyber bullying is *cyber stalking*. Cyber stalking refers to "harassment on the Internet using various modes of transmission such as electronic mail (e-mail), chat rooms, newsgroups, mail exploders, and the World Wide Web." [29]. A study on German SNS StudiVZ, suggested more than 40 % of users experienced cyber stalking at least once with the duration of cyberstalking in some cases lasting more than one year [30].

4.4 How Privacy Risks Manifest

It is also recognized that personal information may be leaked by other means. Maintaining relationship with friends is the main purpose for users joining SNSs. However *online friends* are one of the ways in which individual's personal information becomes exposed. Friends might actively disclose individual's information by posting updates, photograph, events, or tagging photos in SNSs. In this study some participants reported using unfriending strategies in order to preserve their privacy [22]. Others needed to research when they were attacked, for example:

> "Dear Friends, a funny post has been put on my wall by some unknown unscrupulous ….. Kindly ignore, do not open, forward or do anything with it. I am exploring way with FB to take it down. Sorry for any offense it could have caused to you even though am not responsible!!!"

This demonstrates little emphasis on privacy settings in Facebook. Photo tagging in SNSs creates a link from the photo to the person's profile. The decision to tag an individual does not lie with the tagged person but rather to the other party. The tagged person has little or no control about being tagged and may bear damaging implications if it reveals sensitive information of the user [31].

There is evidence from literature to show that users have inadequate knowledge to protect their own privacy. For example, users in Norway were found to have difficulties in understanding and configuring privacy control on OSNs [32]. A study showed that users privacy expectation failed to meet users privacy requirement [33]. Another study in [34] suggested that users did not understand privacy configurations. They discovered that 50 % of the published personal information was shared using default privacy settings and this was not the intention by the majority of the users.

5 Conclusion

This paper reported that participants perceived horizontal risks and no vertical risks. The finding suggests that most of the respondents are aware of privacy risks when using SNSs. The majority of respondents clearly responded towards the horizontal dimension of risks and pointed out several different types of privacy threats for example identity theft, cyber bullying, and information exposure and abuse were highlighted. Some of the risks mentioned could be attributed to the users themselves such as inadequate knowledge for protecting their privacy on SNSs and sharing too much information on SNSs.

These risks are particularly exposed by users' social interaction when interacting online. The risks that emerge out of users' digital activities on SNSs should be made known to them and it is their responsibilities to protect their personal information. Since students perceived the usefulness of SNS for learning purposes, the interplay between privacy concern and participation in learning needs to be addressed in order to encourage students' full and honest participation as students have recognized these tools as being useful for learning purposes.

Students identified horizontal risks without mentioning any of the vertical risks. This would imply that their awareness of possible risks is limited since little information is usually available to them. The limitation of this paper is that the findings are entirely based on the participants' responses in a survey. However, more investigations will be conducted using other qualitative approaches in future.

References

1. Gurses, S., Diaz, C.: Two tales of privacy in online social networks. IEEE Secur. Priv. **11**(3), 29–37 (2013)
2. Boyd, D., Ellison, N.B.: Social network sites: definition, history, and scholarship. J. Computer-Mediated Commun. **13**(1), 23 (2007)
3. Idris, Y., Wang, Q.: Affordances of Facebook for learning. Intl. J. Cont. Eng. Educ. Lifelong Learn. **19**(2), 247–255 (2009)

4. McLoughlin, C., Lee, M.J.: Social software and participatory learning: pedagogical choices with technology affordances in the Web 2.0 era. In: ICT: Providing Choices for Learners and Learning. Proceedings ascilite Singapore 2007 (2007)
5. Bryant, T.: Social software in academia. Educause Q. **29**(2), 61 (2006)
6. Tess, P.A.: The role of social media in higher education classes (real and virtual) – a literature review. Comput. Hum. Behav. **29**(5), A60–A68 (2013)
7. Martin, S., et al.: New technology trends in education: seven years of forecasts and convergence. Comput. Educ. **57**(3), 1893–1906 (2011)
8. Van Dijck, J.: 'You have one identity': performing the self on Facebook and LinkedIn. Media Cult. Soc. **35**(2), 199–215 (2013)
9. Facebook. Statement of Rights and Responsibilities 30 January 2015 [cited 27 March 2015]
10. Jones, A., Martin, T.: Digital forensics and the issues of identity. Inf. Secur. Tech. Rep. **15**(2), 67–71 (2010)
11. Aïmeur, E., Schonfeld, D.: The ultimate invasion of privacy: identity theft. In: 2011 Ninth Annual International Conference on Privacy, Security and Trust (PST). IEEE (2011)
12. Pempek, T.A., Yermolayeva, Y.A., Calvert, S.L.: College students' social networking experiences on Facebook. J. Appl. Dev. Psychol. **30**(3), 227–238 (2009)
13. Price, K.: Web 2.0 and education: what it means for us all. In: Australian Computers in Education Conference (2006)
14. Richardson, W.: Blogs, Wikis, Podcasts, and Other Powerful Web Tools for Classrooms. Corwin Press, Thousand Oaks (2010)
15. Thomas, K., Grier, C., Nicol, D.M.: UnFriendly: multi-party privacy risks in social networks. In: Atallah, M.J., Hopper, N.J. (eds.) PETS 2010. LNCS, vol. 6205, pp. 236–252. Springer, Heidelberg (2010)
16. Dinev, T., Hart, P.: An extended privacy calculus model for e-commerce transactions. Inf. Syst. Res. **17**(1), 61–80 (2006)
17. Debatin, B.: Ethics, privacy, and self-restraint in social networking. Privacy Online, pp. 47–60. Springer, Heidelberg (2011)
18. Bonneau, J., Preibusch, S.: The privacy jungle: on the market for data protection in social networks. Economics of Information Security and Privacy, pp. 121–167. Springer, US (2010)
19. Jones, H., Soltren, J.: Facebook: threats to privacy. In: Project MAC: MIT Project on Mathematics and Computing (2009)
20. boyd, d., Hargittai, E.: Facebook privacy settings: who cares?. First Monday **15**(8) (2010). http://firstmonday.org/ojs/index.php/fm/article/view/3086/2589. Accessed 5 May 2015
21. Yang, Y., et al.: Stalking online: on user privacy in social networks. In: Proceedings of the Second ACM Conference on Data and Application Security and Privacy. ACM (2012)
22. Gundecha, P., et al.: User vulnerability and its reduction on a social networking site. ACM Trans. Knowl. Discov. Data (TKDD) **9**(2), 12 (2014)
23. Lynch, J.: Identity theft in cyberspace: crime control methods and their effectiveness in combating phishing attacks. Berkeley Tech. Law J. **20**, 259 (2005)
24. Campbell, M.A.: Cyber bullying: an old problem in a new guise? Aust. J. Guidance Couns. **15**(01), 68–76 (2005)
25. Albrechtslund, A.: Online social networking as participatory surveillance. First Monday **13**(3) (2008). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949. Accessed 5 May 2015
26. Tokunaga, R.S.: Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships. Comput. Hum. Behav. **27**(2), 705–713 (2011)

27. Lenhart, A., et al.: Social Media & Mobile Internet Use Among Teens and Young Adults. Pew Internet & American Life Project, Washington D.C. (2010)
28. Marwick, A.E., boyd, d.: Networked privacy: how teenagers negotiate context in social media. New Media Soc. **16**(7), 1051–1067 (2014)
29. Deirmenjian, J.M.: Stalking in cyberspace. J. Am. Acad. Psychiatry Law Online **27**(3), 407–413 (1999)
30. Dreßing, H., et al.: Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims. Cyberpsychology Behav. Soc. Netw. **17**(2), 61–67 (2014)
31. Besmer, A., Richter Lipford, H.: Moving beyond untagging: photo privacy in a tagged world. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM (2010)
32. Brandtzæg, P.B., Lüders, M., Skjetne, J.H.: Too many Facebook “friends”? Content sharing and sociability versus the need for privacy in social network sites. Intl. J. Human-Computer Interact. **26**(11–12), 1006–1030 (2010)
33. Madejski, M., Johnson, M.L., Bellovin, S.M.: The failure of online social network privacy settings (2011)
34. Liu, Y., et al.: Analyzing Facebook privacy settings: user expectations vs. reality. In: Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference. ACM (2011)