SOCIAL NETWORKING PRIVACY TOOLS: EASE OF USE AND DEGREE OF CONTROL

Ravi S. Narayanaswamy, University of South Carolina Aiken
Leanne C. McGrath, University of South Carolina Aiken
471 University Parkway, Aiken, SC 29801

ABSTRACT

This research explored the ease of use and degree of control for privacy tools available on social networking sites. Data was gathered from fifty web sites chosen on the basis on their popularity and usage. The number and type of privacy tools available were recorded. Overall, sixty-nine privacy tools were identified and categorized into four types of information, namely profile, personal, social and professional. Ease of use and degree of control were recorded using an applicable seven point Likert scale. In general while privacy tools were relatively easy to locate, there use was a much more arduous task especially for novice users with little knowledge about privacy settings. Additionally regarding degree of control, most privacy tools gave users little to no leverage to customize them to meet their specific needs. As the number of privacy tools for social networking continues to increase, this area of research becomes even more important to the issue of privacy on social networking sites.

INTRODUCTION

Social networking has become a global phenomenon; individuals use it as a landscape to exchange information (Boyd & Ellison 2008). Different types of information such as personal interests, social and professional information are shared in social networking sites (SNS) (Vasalou et al. 2010). In addition, a lot of personally identifiable information is collected during the account sign-up process (Bonneau & Preibusch 2009b). Past trends have shown that the information shared on SNS is vulnerable to many threats (Pilkington 2007). For instance, prospective and current employers (Finder 2006), educational institutions, and other third-party websites (Fogel et al. 2009) use the information on social networking websites for consumer profiling. In some cases it has resulted in damaging consequences for both SNS as well as their users (Rosenblum 2007).

The social networking organizations have been reactive and are increasingly developing several privacy tools to protect user information (Narayanaswamy & McGrath 2012). However, the privacy tools are useful only if the users know to apply them to protect their information. Inasmuch, social networking users are expected to act as system and policy administrators to protect their online content (Ahn et al. 2011). Thus, from a user standpoint it is not only imperative to understand the availability of various privacy controls but also learn how to activate and manipulate them in order to effectively protect their online content.

The main objective of this study is to explore the ease of use and degree of control with respect to various privacy tools available in SNS. The rationale is drawn from the technology acceptance research which contends that individuals intend to use a technology when it requires less effort and is perceived to be beneficial (Venkatesh et al. 2003; Venkatesh et al. 2012). These concepts are captured using ease of use, which refers to the degree of effort required to use the privacy tools, and degree of control, which is the leverage users have to manipulate the privacy tools. The ease of use and degree of control are analyzed for privacy tools available to protect personal, social and professional information. The findings provide

implications for both users and SNS. From a user standpoint, we provide suggestions on the effort required to enable and handle various privacy tools which in turn suggest the extent to which his or her online information can be protected. From a social networking provider perspective, we provide implications on how to enrich various privacy tools in order to cater to user requirements.

BACKGROUND LITERATURE

Research related to social networking is continually emerging. Prior research has explored several issues related to social networking. For instance, a large body of research has focused on examining the factors that motivate individuals to participate in social networking (Boyd & Ellison 2008; Tufekci 2008). Another stream has explored user attitudes towards social networks with an emphasis on information sharing and disclosure (Constant et al. 1994; Livingstone 2008). Similarly some recent works have analyzed the relationship between cultural affiliation and social networking (Fogg & Iizawa 2008; Vasalou et al. 2010).

Specifically, research exploring social networking privacy issues has largely explored it from a technical perspective, i.e., how technical configurations can be enhanced to protect user privacy (Bonneau et al. 2009a; Huber et al. 2011). For instance, previous research has examined the content of privacy policies (Bonneau & Preibusch 2009b) and has analyzed the potential threats and risks of using social networking (Dwyer et al. 2007; Frankowski et al. 2006). A common agreement among most of the studies is that information shared on social networking sites is subject to various attacks that include spam, phishing and identity theft (Gross & Acquisti 2005; Huber et al. 2011; Jones & Soltren 2005). These studies depict the ease of extracting information from social networking sites. For instance, attackers could take photographs extracted from a friend's social networking pages and use them as personal signatures to create an authentic phishing message (Jagatic et al. 2007). The burden to protect online content is skewed towards the user rather than the social networking site (Dwyer et al. 2007). In other words, users must employ the privacy tools in order to protect their online content. Thus it is imperative to understand the factors that will trigger the user's intention to accept and use the privacy tools.

The technology acceptance and use literature contends that individual's intention to accept and use a technology is influenced by four key factors: effort expectancy, performance expectancy, social influence and facilitating conditions (Venkatesh et al. 2003; Venkatesh et al. 2012). Performance expectancy is defined as the degree to which using a technology will provide benefits to individuals in performing certain activities; effort expectancy is the degree of ease associated with individuals' use of technology; social influence is the extent to which individuals perceive that important others (e.g., family and friends) believe they should use a particular technology; and facilitating conditions refer to individuals' perceptions of the resources and support available to perform a behavior (Brown & Venkatesh 2005; Venkatesh et al. 2003; Venkatesh et al. 2012). In particular, this study extends two constructs to social networking privacy and contends that individuals' intention to use a privacy tool will depend upon the extent to which it is easy to deploy and the extent to which they can leverage it to maximize the benefits. To illustrate, an app installed by a user's friend could have access to the user's information even if the user does not install the app himself or herself (Barbara 2011). Even though it is possible for the user to opt out of sharing information with his or her friends' apps, many users "do not know to do this because they are not aware that the sharing is happening in the first place" (Barbara 2011). From a broader perspective, a privacy tool is beneficial only if the user can customize it to meet his or her requirements to protect his or her online content.

METHOD

A list of major social networking sites collected from Alexa, a web information company, as a part of a larger project was used to capture the ease of use and degree of control for each privacy tool. The sites

chosen in this study are consistent with prior research (e.g., Bonneau et al. 2009b) examining user privacy in social networking sites. In addition, these sites were examined to ensure accessibility and authenticity. Data was collected by one individual to ensure consistency of ratings. Following this, a generic user account was created to gain access into the social networking site and examine the privacy tools available to protect different types of user information. First, all the privacy tools available on each social networking site were recorded; overall a total of sixty-nine privacy tools were identified. Second, the ease of use and degree of control were examined for each privacy tool and coded using a seven point Likert scale. The scale for ease of use was (1 -- Extremely easy, 2 – Very easy, 3 – Easy, 4 – Somewhat easy, 5 – Difficult, 6 – Very difficult, 7 – Extremely difficult). Factors such as effort required to locate the tool and appearance (icon, text) were taken into consideration while determining the ease of use. Similarly, the scale for degree of control was (1 – Extremely customizable, 2 – Very customizable, 3 – Customizable, 4 – Somewhat customizable, 5 – Little customizability, 6 – Very limited customizability, 7 – Extremely limited customizability). Factors such as number of options, for example public, private, by invitation only, among others were taken into account to determine the degree of control. This was done for all the sixty-nine privacy tools.

RESULTS & DISCUSSION

Overall the social networking sites provided a wide array of privacy tools for users to protect their online content. However, most of the privacy tools have to be enabled manually. More interestingly, it was the user's responsibility to make sure the privacy tools remains active; it was not a one-time task. The SNS included in this study are listed in Table 1.

Table 1. Top Social Networking Sites

	Social Networking Site	**Category**
1.	Facebook	General-Purpose
2.	MySpace	Gaming
3.	Twitter	Micro-blogging
4.	Bebo	General-Purpose
5.	Habbo	General-Purpose
6.	Tagged	General-Purpose
7.	Okrut	General-Purpose
8.	Friendster	General-Purpose
9.	Badoo	General-Purpose
10.	LinkedIn	Business-Networking
11.	Hi5	General-Purpose
12.	NetLog	General-Purpose
13.	Flixster	Media recommendation
14.	MyLife	Reunion
15.	Classmates.com	Reunion
16.	Last.fm	Media recommendation
17.	Viadeo	Business-Networking
18.	WeeWorld	Gaming
19.	Xanga	General-Purpose
20.	GaiaOnline	Gaming

21.	SkyRock	General-Purpose
22.	MyYearbook	General-Purpose
23.	BlackPlanet	General-Purpose
24.	Fotolog	Photo-blogging
25.	FriendsReunited	Reunion
26.	LiveJournal	General-Purpose
27.	meinVZ	General-Purpose
28.	Sonico	General-Purpose
29.	Plaxo	General-Purpose
30.	StumbleUpon	Media recommendation
31.	Multiply	General-Purpose
32.	Hyves	General-Purpose
33.	BuzzNet	Media recommendation
34.	WAYN	Travel
35.	Care2	General-Purpose
36.	DeviantART	Media recommendation
37.	XING	Business-Networking
38.	MyOpera	Blogging
39.	OpenDiary	Blogging
40.	Livemocha	Language Learning
41.	weRead	Media recommendation
42.	ibibo	General-Purpose
43.	MocoSpace	General-Purpose
44.	CouchSurfing	Travel
45.	Nexopia	General-Purpose
46.	PerfSpot	General-Purpose
47.	Yonja	General-Purpose
48.	Bahu	General-Purpose
49.	Eons	General-Purpose
50.	ExperienceProject	Privacy-Specific

Table 2 shows the distribution of privacy tools related to profile, personal, social and professional information.

Table 2: Summary of Information Types and Associated Privacy Tools

Type of Information	**Number of Privacy Tools**
Profile Information	22
Personal Information	24
Social Information	13
Professional Information	10

Table 3. Privacy Tools Ease of Use		
Information Category	**Average Scores**	**Standard deviation**
Profile	1.31	0.43
Personal	1.39	0.45
Social	1.15	0.26
Professional	1.58	0.57

Overall most of the privacy tools were fairly accessible; the ease of use average scores listed in Table 3 indicate that most of the privacy tools were easy to locate and activate. However, some privacy tools were easier to locate compared to others. For instance, privacy tools related to social information were apparent and could be easily activated. This is consistent with the existing trends which reveal that individuals increasingly use SNS to share social information such as photos and friendly blogs (Bonneau & Preibusch 2009b). On the other hand, privacy tools for professional information were a little harder to locate. These trends were common across most of SNS with little or no variation.

Table 4. Privacy Tools Degree of Control		
Information Category	**Average Scores**	**Standard deviation**
Profile	5.01	1.48
Personal	4.88	1.96
Social	4.66	2.23
Professional	4.11	2.31

The average scores for degree of control listed in Table 4 indicate low customization of privacy tools. In general most privacy tools provided little or no leverage for users to customize them to meet their needs. Most common option was “private” or “public”. Some of the major SNS like Facebook provided more options allowing users to specify who is able and not able to view the shared content. However, it was done for a narrow range of privacy tools. Surprisingly, privacy controls related to profile information had the lowest level of customization. For instance, the profile name and photo were always shown with no option to hide the visibility. This reiterates the point about the increasing growth in social phishing i.e., using photos on SNS to create authentic phishing messages (Jagatic et al. 2007). Moreover, some of the options for the user were stressful and very confusing. Users must be well versed with the terminology to determine the best way to protect their online content. While major SNS players like Facebook are making changes to their design and features to provide users more control over their information, most of them are still in trial and error mode.

Overall the findings imply that privacy in SNS is still emerging and does not offer complete protection of online data. With users sharing more information on social networking sites, these sites become an attractive target for both legal and illegal bodies (Boyd & Crawford 2011). More importantly, SNS users no longer have to worry just about what Facebook, Google+, LinkedIn and other social sites do with their database information; they have to worry about what SNS can enable others to do with it also. For example, organizations are using Facebook as a potential database for retrieving photos which in turn are used for consumer profiling (Chunka 2011). The surprising part is that no login was required to collect basic user information. While the privacy tools were easy to locate, applying them in the right manner was a horrendous task. There is a large learning curve for employing privacy tools; this is especially true for novice users (Vaknin 2011). As a SNS user, it is important to pay close attention to the details about

different types of privacy tools. The users must educate themselves about the privacy settings before uploading the information. SNS like Facebook are developing rich knowledge bases to educate users about privacy settings (Eldon 2011). The privacy paradox plaguing SNS is waning; it is time that users bore some responsibility for their actions.

In summary, while the SNS allow users to share different types of information, it is important for users to exercise some judgment to determine which information is safe on the social networking site. The SNS are deploying privacy tools at an increasing rate; however, not of all them are useful to protect online content. Most interestingly, the users must learn how to use the privacy tools in the correct manner failing which the privacy tool itself does not offer much help.

CONCLUSION

Privacy issues in social networking are a work in progress that urges the need for more research in identifying new solutions to protect user information. While the social networking sites are introducing new privacy tools to protect user information, not many of them can be fully leveraged. In other words, privacy tools were easy to locate and activate but customizing to meet specific needs was almost impossible. Future research can extend the findings presented in this study to explore how privacy tool ease of use and degree of control affects the quality of user information shared on SNS. This research hopes that the ideas presented here, along with the ease of use and degree of control findings, will be an important starting point towards enhancing privacy in SNS.

REFERENCES

Ahn, G.-J., Shehab, M., and Squicciarini, A. (2011) Security and Privacy in Social Networks. *IEEE Internet Computing* 15(3), 10-12.

Barbara, O. (2011) Q and A: Facebook Privacy Changes, in: *Technology*. USA Today, New York.

Bonneau, J., Anderson, J., and Danezis, G. (2009a) Prying Data out of a Social Network. Advances in Social Networks Analysis and Mining.

Bonneau, J., and Preibusch, S. (2009b) The Privacy Jungle: On the Market for Data Protection in Social Networks. *WEIS 2009 The Eighth Workshop on the Economics of Information Security*) 1-45.

Boyd, D. M., and Crawford, K. (2011) Six Provocations of Big Data. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, Oxford Internet Institute.

Boyd, D. M., and Ellison, N. B. (2008) Social Networking Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication* 13, 210-230.

Brown, S. A., and Venkatesh, V. (2005) Model of Adoption of Technology in the Household: A Baseline Model Test and Extension Incorporating Household Life Cycle. *MIS Quarterly* 29(4), 399-426.

Chunka, M. (2011) Facebook's Privacy Issues Are Even Deeper Than We Knew. *Forbes*.

Constant, D., Kiesler, S., and Sproull, L. (1994) What's Mine Is Ours, Is It? A Study of Attitudes About Information Sharing. *Information System Research* 5(4), 400-423.

Dwyer, C., Hiltz, S. R., and Passerini, K. (2007) Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace. Thirteenth Americas Conference on Information Systems.

Eldon, E. (2011) Analysis: Some Facebook Privacy Issues Are Real, Some Are Not. *Inside Facebook.*

Finder, A. (2006) For Some, Online Persona Undermines a Resume. *The New York Times*, June.

Fogel, J., and Nehmad, E. (2009) Internet Social Network Communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153-160.

Fogg, B. J., and Iizawa, D. (2008) Online Persuasion in Facebook and Mixi: A Cross-cultural Comparison. Persuasive, 35-46.

Frankowski, D., Cosley, D., Sen, S., Terveen, L., and Riedl, J. (2006) You Are What You say: Privacy Risks Of Public Mentions. 29th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, ACM, New York, 565-572.

Gross, R., and Acquisti, A. (2005) Information Revelation and Privacy in Online Social Networks (The Facebook Case), Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, 71-80.

Huber, M., Mulazzani, M., Kitzler, G., Goluch, S., and Weippl, E. (2011) Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam. *IEEE Internet Computing,* 15(3), 28-34.

Jagatic, T., Johnson, N., Jakobsson, M., and Menczer, F. (2007) Social Phishing, *Communications of the ACM* 50(10), 94-100.

Jones, H., and Soltren., J. (2005) Facebook: Threats to Privacy. *Project MAC: MIT Project on Mathematics and Computing*.

Livingstone, S. (2008) Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy, and Self-expression. *New media & society,* 10(3), 393-411.

Narayanaswamy, R., and McGrath, L. (2012) Social Networking: Privacy Control Tool Availability and User Characteristics. 42nd Southeast Decision Sciences Annual Meeting, Columbia, SC, February.

Pilkington, E. (2007) Blackmail Claim Stirs Fears Over Facebook. *The Guardian,* 16, July.

Rosenblum, D. (2007) What Anyone Can Know: The Privacy Risks of Social Networking Sites. *IEEE Security & Privacy Magazine* 5(3), 40.

Tufekci, Z. (2008) Grooming, Gossip, Facebook and Myspace: What Can We Learn About These Sites From Those Who Won't Assimilate? *Information, Communication,and Society* 11(4), 544-564.

Vaknin, S. (2011) How To Protect Your Facebook Timeline Privacy. *CNET How to*, CNET.

Vasalou, A., Joinson, A., and Courvoisier, D. (2010) Cultural Differences, Experience with Social Networks and the Nature of "True Commitment" in Facebook. *International Journal of Human Computer Studies* 68(10), 719-728.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003) User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly* 23(3), 425-478.

Venkatesh, V., Thong, J. Y. L., and Xin, X. (2012) Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly* 36(1), 157-178.

Acknowledgment: This work is partially supported by a grant from the USC Magellan Scholar program. A special thanks is given to the Magellan Scholar for data collection.