

SOCIAL NETWORKING AND PRIVACY: THE DICHOTOMY

Leanne C. McGrath, University of South Carolina Aiken, 471 University Parkway, Aiken, SC

ABSTRACT

Millions of people use social networking sites daily to communicate with others. The protection of their personal information has raised many concerns about privacy. This paper discusses the actual privacy statements of several social networking sites and reports on their adherence to the five globally accepted fair practices for privacy policies.

INTRODUCTION

In today's technologically savvy society, the use of the Internet for social networking has become more and more popular for communication among friends, business partners, and many other individuals. These sites are especially popular among young adults and teenagers.

Social networks basically consist of nodes (people) and ties (connections or relationships between and among those people). Specifically, Turban et. al. define social networks as places "where people create their own space, or home page, on which they write blogs (web logs), post pictures, videos or music, share ideas, and link to other Web locations they find interesting" [11, p. 822].

Overall, the public nature of information shared on social networking sites has raised legitimate concerns for privacy issues. This paper provides some background about social networks, and then it focuses to examine one particular area of privacy, namely the privacy policies posted on several targeted social networking web sites.

BACKGROUND

The dawn of social networks has just passed its milestone 10th year. SixDegrees.com is credited as the first site recognizable as a social network. It began in 1997 and had a rather short life when, in 2000, it failed to sustain itself as a business and thus closed [2].

The next social networking wave began in 1999 with LifeJournal, AsianAvenue, and BlackPlanet. A few new sites appeared in 2000 through 2002. Then in 2003 several social networking sites, including MySpace and LinkedIn launched. In 2005 Yahoo! 360, YouTube, and Facebook (the high school networks) were a few of the more popular social networking sites that began. Finally in 2006, Windows Live Spaces, MyChurch, Facebook (corporate network) and Facebook (everyone) were launched [2].

The popularity of social networks is growing at a very rapid rate globally. For example, in a scant two years, MySpace gained over fifty million members [3]. Online profiles for users typically contain a myriad of personal information, including name (or pseudonym), age (or birthday), hometown, interests, "about me," and photographs. They can also include religion, ethnicity, and any other identifying

information about the person. All this information is willingly and knowingly uploaded by the individual member. The visibility of a user's profile information varies by web site and at the discretion of the user. As members, users are urged to identify other persons in the system with whom they have a relationship, defined loosely with various categories such as Friends, Contacts, Followers, or Fans [2]. Research from the Pew Internet & American Life Project states that 91 % of teens in the United States who use social networking sites do so to connect and socialize with their friends, and 49% of users say they do so to make new friends [8]. Overall, social networks create differentiation by structural differences regarding visibility and access [2].

The visibility and access to personal information, characteristic of social networking web sites, raises the issue of privacy. As millions turn to these sites for social relationships, serious concerns about privacy have emerged. Some of these areas include identity theft, attraction of sexual predators, governmental data collection, marketers' use of information, college admission use, school usage, and employer or future employer utilization of information from these sites. For example, schools have disciplined students who make derogatory statements about teachers or show pictures of inappropriate student behavior. Beyond these consequences, students may be putting their reputations and their future careers in jeopardy. Many wonder how a generation so Internet savvy can be so naïve concerning the issue of their privacy [6].

Marketers can gather personal information from social networking sites and use it for purposes beyond that which the social network user intended. For instance, the personal information can be used for commercial purposes [1]. The threat of sexual predators online already has some facts to substantiate the claim. In Connecticut, police reported that several girls had been sexually assaulted by men that they met on a social networking site [3]. Survey data has shown that a complete stranger has contacted 43% of teens on social networking sites. Also 31% of the teens reported having individuals listed as friends on their social networking profile despite the fact that they had never personally met them [8]. This could be a potentially fatal danger for unsuspecting youths.

Employers are using social networks to gather both insights about prospective employees and to learn about or monitor existing employees. Inappropriate words and pictures on a social network, if viewed by a prospective employer, can portray an image of a candidate that is less than desirable and thereby affect his or her chances of being offered a job. Of course time spent in social networking while at work can lead to a decrease in employee productivity. If the social networking is being done for business purposes, this should be limited to certain employees and have a time limit per day for instance. Corporate sales have been claimed to increase through social networking. If the purpose of the social networking is to exchange professional information, then corporate secrets must be protected with clear guidelines concerning this issue. Overall, corporate policies addressing all aspects of social networking by employees will help to improve the effectiveness of using such sites [9].

And finally, it has been recognized that social networks need privacy policies that provide the same social privacy protection online that is found offline, given that most offline social transactions do not leave a trace [5]. The importance of this issue cannot be overlooked or overstated.

RESEARCH METHOD

The number of online social networks is in the hundreds. Since this is a pilot study, the sample analyzed for this paper includes only a few of the most notable social networking sites rated by popularity. Specifically, to be chosen for review, the sites had to have at least 10,000,000 registered users, have open registration, and not be primarily based in countries outside the United States. The overall list of social

networking sites was obtained from Wikipedia in April 2008 and contained 118 web sites [12]. After narrowing the sites, seven privacy statements were analyzed. These social networking sites are the most popular, and thus their privacy practices are assumed to give valuable insight about the actual privacy afforded most social networking users.

The globally recognized components essential for an effective online privacy policy are Notice, Choice, Access, Security, and Enforcement. Since these are the globally accepted primary fair practices, compliance with them will be the focus of this study. Each one of these elements provides a dimension of privacy protection for the user. Specifically, the five areas are defined below.

Notice informs the user what information is gathered, how it is used, and whether the site shares the information with others.

Choice declares whether the user is allowed a voice in the amount of information gathered and how that information may be used.

Access deals with providing the user a means to review collected data and correct it if needed.

Security refers to how information is safeguarded, along with other issues relating to integrity of information and to the site's computer related practices.

Enforcement relates to consequences imposed for breach of the fair practice elements [7][4][10].

RESULTS AND DISCUSSION

Each element of the fair practices, recognized universally as essential to a privacy policy, was evaluated for the social networking sites that comprise the pilot sample. The specific sites analyzed and their number of registered users are in Table 1 below.

TABLE 1: SOCIAL NETWORKING WEB SITES IN PILOT SAMPLE

Name	Registered Users
Classmates.com	40,000,000
Facebook	97,800,000
Imeem	16,000,000
LinkedIn	20,000,000
MySpace	110,000,000
Tagged.com	30,000,000
WindowsLiveSpaces	40,000,000

Of these, it can be seen that Facebook and MySpace are extremely popular social networking sites. Overall, each social networking site had a privacy statement link on its home page. Regarding Notice, each one told the user what online information was collected and how that information was used. Table 2 below gives the items commonly listed as collected in the privacy policies.

TABLE 2: COMMONLY COLLECTED INFORMATION

Name
Address
Phone Number
e-Mail Address
IP Address
Credit Card Number
Site uses information to make a user personal profile
Site tracks information about pages the user visits

Classmates.com and Windows Live Spaces collected all of these items. The social networking site, imeem.com, declared collection of the fewest number of items, specifically address, e-mail address, and IP address. Four of the sites asked for one’s birthday, and another one asked directly for one’s age. Notice of other information collected on one or more social networking sites included gender, marital status, community affiliations, hobbies, schools, lifestyle, eye color, personality type, social security number, driver’s license number, sports, food, and TV shows. If a user gives all this information, certainly a revealing personal profile can be established, and a generous measure of privacy lost even to the point of possible informational use for identity theft. It is also prudent to point out that all sites, except LinkedIn, stated that information was collected in the “such as” format, and thus disclosure of types of information was not exhaustive. Some sites just chose to reveal more of what was collected than others did. Only Classmates.com specifically stated that the user was no longer anonymous since information was publicly displayed and could appear in search engines. MySpace.com, Windows Live Spaces, and Classmates.com also gave Notice that they can supplement information given by the user with information received from third parties. Facebook.com declared that it may collect information from other sources such as newspapers, blogs, and instant messaging.

All of the sites told the user how their information is shared. As expected, all sites stated that information was shared in response to requests from the law. All except imeem.com stated sharing with partners, and all but Classmates.com declared sharing in order to protect the site and its interests. Furthermore, four social networking sites, specifically Classmates.com, imeem.com, Tagged.com, and LinkedIn.com, stated that no individually identifiable information is shared with any third party. Finally, all sites discussed privacy relating to children. They either declared compliance with the Children’s Online Privacy Protection Act or stated that the site does not knowingly collect information from children. One site, Classmates.com, declared both.

The issue of Choice was somewhat difficult to discern in some of the privacy policies. This element deals with whether a user has a “say” in how their information is used. No social networking site declared total user control of their personal information. This issue could be classified as a “partial say” when it only provides an opt-out choice regarding e-mail promotions, e-mail address sharing, or how the site communicates with the user. Only MySpace.com declared an opt-out of information collection by other companies. And imeem.com did not directly address the issue of Choice.

In aggregate, the coverage of the element of Choice was rather discouraging. When addressed in the privacy policy, it really only provided the user with a “partial say” to opt-out of very limited areas that basically involved business communication and promotion. And although MySpace.com declared an opt-out choice for collection of information by other companies, nothing was addressed on any of the social networking sites to stop the selling of personal profile information to outside companies. Some

information was mandated in order to use the respective site, and this somewhat negates the issue of Choice other than the option to not use the site.

By the very nature of social networking sites, the user has Access to view the information collected and stored about him or her. Additionally, the member has an online means of correcting inaccuracies in the information collected about him or her. One site, Facebook.com, additionally stated that changed information might exist in backup copies for a reasonable time although the exact length of that time was not declared.

Three of the social networking web sites clearly stated that they could not guarantee 100% Security, and four included a statement that reasonably ensured security and integrity of information collected by appropriate industry practices. However, little elaboration of provisions with specific details was given. One item that all sites did declare was the use of “cookies,” with five sites stating persistent “cookies” were placed. All but one site, LinkedIn.com, told users that their browser could be set to reject “cookies.” Third party “cookies” were allowed for placement by all of the social networking sites. Finally, there was very spotty information about storage and transmission of information, a vitally important area by the very nature of social networks. Only Facebook.com and imeem.com declared storage of information on a secure server. Five web sites, excluding MySpace.com and Tagged.com, stated the use of Secure Socket Layers (SSL) to transmit information.

And finally the element of Enforcement is reported. The social networking sites, Classmates.com, Facebook.com, Windows Live Spaces, and LinkedIn.com, acknowledged enforcement by self-regulation and by use of TRUSTe, an independent, non-profit organization, as recourse for unresolved issues regarding privacy practices. In actuality, however, all web sites can be held to their posted privacy statement, whether it specifically mentions Enforcement or not.

In summary, web sites need to pay attention to all five elements of fair practices for privacy statements. For social networking web sites this presents a dichotomy because of the very nature of information sharing done to establish relationships via these web sites. From this pilot study of assessment of the actual privacy statements currently in use, some social networks protect privacy better than others do. Users beware definitely holds true. There are choices as to which social network to join. A strong message concerning the importance of privacy would be sent if users become informed and choose those social networking web sites that offer the best protection of their privacy.

CONCLUSION

There is no way around the issue of privacy when personal information about people is at the center of social networking sites. This pilot study regarding privacy statements and their adherence to the globally accepted fair practices, namely Notice, Choice, Access, Security, and Enforcement, focuses the spotlight on what these sites are currently doing to meet the standards. All the social networking sites reviewed could improve their respective privacy statements to achieve full compliance to the five standards.

Privacy must be addressed in a satisfactory manner to protect those using the social networking web sites. The concept of privacy and its protection is a challenging legal issue today for these sites. As technology pushes the envelope, much is to be learned and defined in the future relating to social network visibility, access to personal information and the protection of privacy while using social networking web sites.

REFERENCES

- [1] Barnes, S. "A Privacy Paradox: Social Networking in the United States." *First Monday*, 2006, 11(9). Retrieved April 23, 2008 from http://www.firstmonday.org/issues/issue11_9/barnes/index.html
- [2] Boyd, D. M., and Ellison, N.B. "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-mediated Communication*, 2007, 13(1), article 11. Retrieved April 22, 2008 from <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>
- [3] Consumer Affairs. "Connecticut Opens MySpace.com Probe." *Consumer Affairs*, 2006, February 5. Retrieved April 28, 2008 from <http://www.consumeraffairs.com/news04/2006/02/myspace.html>
- [4] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995)," Retrieved July 28, 2008 from http://www.cdt.org/privacy/eudirective/EC_Directive
- [5] Dwyer, C., Hiltz, S.R., and Passerini, K. "The Benefits of Facebook "Friends": Exploring the Relationship Between College Students' Use of Online Social Networks and Social Capital." *Proceedings of AMCIS 2007*, Keystone, CO, 2007. Retrieved April 23, 2008 from <http://csis.pace.edu/~dwyer/research/DwyerAMCS2007.pdf>
- [6] Kornblum, J., and Marklein, M.B. "What You Say Online Could Haunt You." *USA Today*, 2006, March 8. Retrieved April 23, 2008 from http://www.usatoday.com/tech/news/internetprivacy/2006-03-08-facebook-myspace_x.htm
- [7] *Federal Trade Commission Report*. "Privacy Online: A Report to Congress," June 1998, the Internet, <http://ftc.gov/reports/privacy3/pri23a.pdf>.
- [8] Lenhart, A., and Madden, M. "Teens, Privacy & Online Social Networks." *Pew Internet and American Life Project Report*, 2007, April 18. Retrieved April 23, 2008 from http://pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf
- [9] Perkins, B. "The Pitfalls of Social Networking." *Computerworld*, 2008, February 11, 42(7), 44.
- [10] "Privacy Basics: The OECD Guidelines, 1980." Retrieved July 28, 2008 from <http://www.cdt.org/privacy/guide/basic/oecdguidelines>
- [11] Turban, T., King, D., McKay, J., Marshall, P., Lee, J., and Viehland, D. *Electronic Commerce 2008 A Managerial Perspective*, Prentice Hall, 2008.
- [12] Wikipedia Foundation INC. (2008). Wikipedia. Retrieved April 4, 2008, http://en.wikipedia.org/wiki/List_of_social_networking_websites