3-1-2009

Social Network Privacy: Expectations vs Reality

Paul H. Schwager
schwagerp@ecu.edu

Bryan C. Foltz

SOCIAL NETWORK PRIVACY: EXPECTATIONS VS. REALITY (RESEARCH IN PROGRESS)

C. Bryan Foltz
University of Tennessee at Martin
foltz@utm.edu

Paul H. Schwager
East Carolina University
schwagerp@ecu.edu

ABSTRACT

This study is an initial step in a larger study which explores issues associated with security and privacy in social network sites (SNSs). Sites such as Facebook, MySpace, LinkedIn, Bebo, Ning and others have increased in popularity and are receiving increased attention from industry and academics as SNSs move beyond the youth market. Most SNSs are targeted towards individuals, yet they are impacting organizations and will change the way business is conducted in the future. Utilizing a survey of MBA students from two US institutions, this study explores the issue of privacy and proposes a model which addresses the risks, expectations, and reality of social networking privacy. It also outlines an agenda for future research.

Keywords

Social Networking, Social Networks, Facebook, MySpace, IS Security, IS Privacy

INTRODUCTION

The use of social network sites (SNSs) is growing rapidly. Although the concept is not new, the popularity and widespread use of these sites is. Along with this explosion in popularity has come an explosion in security concerns. Although most social network sites provide users with numerous privacy controls, most users simply accept the default settings. Since most social network sites rely on accurate data to help individuals connect with friends, users are encouraged to submit accurate data. Unfortunately, much of this data is available for anyone to see. This paper will address this initial phase of a larger study. The purpose of this initial phase is to compare user expectations of privacy within social networking sites to the privacy actually achieved by these sites. In addition the associate issue of security will also be explored.

REVIEW OF RELEVANT LITERATURE

Boyd and Ellison (2007) define SNS as web-base systems which allow individuals to: 1) create public or semi-public profiles within a bounded system, 2) identify a list of individuals as shared connections, and 3) the ability to view and move amongst these connections as well as others in the system. This definition carefully avoids the use of the term networking, which can imply relationship initiation and is not the intention of these sites (Boyd and Ellison, 2007). Furthermore, Boyd and Ellison (2007) provide an excellent overview of the history and development of social network sites, which provides an excellent background the current study.

Current Uses of Social Networking

Although social networking sites exist primarily to help individuals connect with one another, many innovative uses of these tools exist. For example, Skiba summarizes the use of Twitter in the classroom (Skiba, 2008) and suggests that it can be used to support "active, interactive, and reflective learning". Carter, Foulger, and Ewbank (2008) suggest that the use of SNSs can allow teachers to establish more powerful and deeper relationships with students and may enhance communications with shy or less outgoing students. In addition, SNSs have frequently been used to promote clubs or other social groups (Carter, Foulger, and Ewbank, 2008). Social networks are also being used by employers to evaluate potential employees and internship positions (Peluchette and Karl, 2008).

Social Network Privacy Expectations

Users expect the social networking sites to protect their data.

Users expect social networking sites to protect their data. Since these networks support friendships, users assume they can exchange privileged data with their friends without regard for security (Felt and Evans, 2008). Some social networking sites require information such as a college email account to join. These requirements can increase expectations of privacy by appearing to suggest that users share a physical community, thus increasing users' sense of trust in the network (Gross and Acquisti, 2005). Finally, the terms of service of the various social networking sites encourages users to only publish accurate information within their profiles (Gross and Acquisti, 2005).

Social Network Privacy Reality

Users often publish vast amounts of private information that is often published online without restriction.

Although most SNSs suggest users not disclose personal information online, many users seem quite happy to do so (Gross and Acquisti, 2005). In fact, a 2005 survey revealed that over 90% of analyzed profiles contained photographs of the users, almost 88% included a birth date, almost 50% included an address, and almost 40% included a phone number (Gross and Acquisti, 2005). Since most of these profiles are identified by full name, an amazing amount of information is being voluntarily disclosed against the recommendations of the sites themselves (Gross and Acquisti, 2005). A later survey conducted by Goettke and Christiana (2007) reports similar releases of private data.

Essentially, users seem unaware of the volume of information they are providing to people they do not know (Goettke and Christiana, 2007). Further, many users are willing to share this personally identifiable data with strangers--an action they would not consider in real life (Goettke and Christiana, 2007). This willingness to share private data may result from a lack of awareness. Gross and Acquisti suggest that SNS users may not realize how many people can view their data, and may also not understand the consequences of letting others view this private data.

Despite the publication of large amounts of private data, users typically don't change default security settings.

Since most sites default to publically displaying data, private data may be released to the world. Since social networking sites do collect vast amounts of data, such sites typically provide users with tools to prevent the release of this data (Felt and Evans). Unfortunately, most users do not bother changing the default settings, instead simply trusting the social networking site to make proper choices for them (Gross and Acquisti, 2005).

Carter, Foulger, and Ewbank (2008) make an interesting comparison between social networking sites and “old fashioned party line telephones” but note one important difference: SNS are far more permanent than any telephone conversation. The recent change (and subsequent restoration) of Facebook’s terms of service to allow the company permanent use of all posted material is an excellent example (Singel, 2009).

Public Posting of Private Data: An Explanation

This research serves as the initial step in a larger study which will explore reasons why users post personal data online. This behavior will be examined using Ajzen’s Theory of Planned Behavior (1998), along with expansions proposed by Foltz, Schwager, and Anderson (2008). The Theory of Planned Behavior (TPB) predicts and explains human behavior within specific contexts (Ajzen, 1991). The TPB suggests that behavior is best predicted by examining individual intention to commit that behavior (Beck and Ajzen, 1991). Further, intentions are formed from three constructs: attitudes toward the behavior, subjective norms, and perceived behavioral control (Ajzen, 1988). Attitudes toward the behavior reflects the individual’s evaluation of the behavior (Ajzen, 1988; Doll and Ajzen, 1992). Subjective norms is an indication of social pressure from referent others to perform (or not perform) the behavior (Ajzen, 1988). In other words, subjective norms reflect peer pressure (Doll and Ajzen, 1992). The third factor contributing to the formation of intentions is perceived behavioral control. Perceived behavioral control reflects a person’s perception of factors that influence their control over the behavior in question (Ajzen, 1988). Perceived behavioral control also directly influences behavior (Ajzen, 1988).

The TPB does not explicitly consider individual knowledge of technical areas. However, individuals may elect to trust other experts to make decisions for them (Earle and Cvetkovich, 1995). This willingness to rely on others who know (or are perceived as knowing more) about a given area is known as social trust (Siegrist, Cvetkovich, and Roth, 2000).

Apathy may be another factor in understanding why people post data online without protecting their privacy. Apathy has been identified as a lack of motivation, interest, and emotion (Robert et al, 2002). A previous study by Foltz, Schwager, & Anderson (2008) revealed that apathy was indeed useful in explaining why users did or did not read computer usage policies. In short, users may simply not care about their privacy on SNSs.

RESEARCH QUESTIONS

Several questions need to be understood before exploring the issues of SNS privacy and security in greater depth. First we must establish that overall SNS users are concerned about these issues and it is a relevant topic to explore.

RQ1p: SNS users are concerned about SNS privacy issues

RQ1s: SNS users are concerned about SNS security issues

Because age has been associated with the use of SNSs, we believe that younger SNS users will be less sensitive to privacy and security issues.

RQ2p: Older SNS users will be more concerned about SNS privacy issues than younger users

RQ2s: Older SNS users will be more concerned about SNS security issues than younger users

Because many users are unaware of their privacy and security exposure through SNSs, we believe there will be a significant difference between user expectations and reality.

RQ3p: User expectations of SNS privacy issues is greater than SNS actual privacy

RQ3s: User expectations of SNS security issues is greater than SNS actual security

Understanding these basic questions is an important first step before continuing to the next stages of the overall study.

RESEARCH PLAN

This study will be in the data collection phase during January 2009 with initial results being reviewed in February. It will utilize a web-based survey that will be distributed to MBA students at two US academic institutions. It is hoped that by using MBA students we will address a broad section of users that include various ages and backgrounds. The survey will include questions that address users' privacy and security expectations of SNSs as well as their understanding of SNS policies.

DIRECTIONS FOR FUTURE RESEARCH

The complete study will include all elements of the Ajzen's (1988 & 1991) Theory of Planned Behavior (TPB) as well as the additional dimension of apathy indentified by Foltz, Schwager, & Anderson (2008).

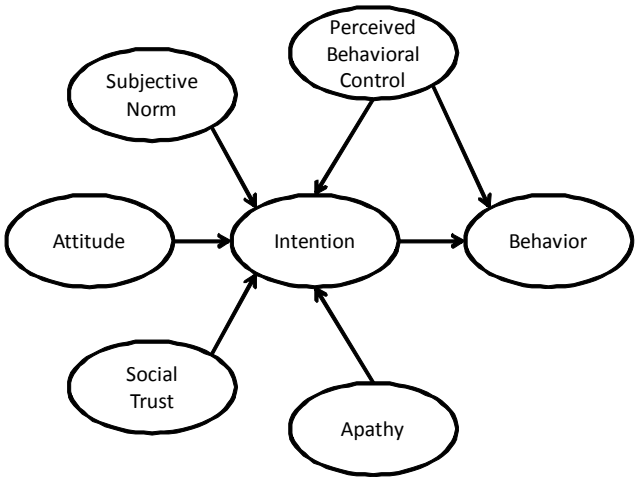

Figure 1. TPB Extended (Foltz, Schwager, and Anderson 2008)

We believe that the TPB extended model will prove useful in understanding users' expectations as well as actual behaviors. Specifically we believe that the Apathy variable will be significant.

CONCLUSIONS

This study is clearly a work in progress. To date the vast majority of research has focused on social networking and the younger generations. This study moves beyond this limitation and extends to other age groups which are also beginning to participate in SNSs in greater numbers. The study will also explore the levels to which users are concerned about and pay attention to SNS privacy and security issues as well as the reasons for these concerns of lack thereof.

Results from the initial data collected will be presented at the conference as well as preliminary insights into the issues identified from the open ended questions.

REFERENCES

1. Ajzen, I. (1988) *Attitudes, Personality, and Behavior*, The Dorsey Press, Chicago, IL.
2. Ajzen, I. (1991) The theory of planned behavior, *Organizational Behavior and Human Decision Processes*, 50, 2, pp. 179-211.
3. Beck, Lisa and Icek Ajzen. "Predicting Dishonest Actions Using the Theory of Planned Behavior." *Journal of Research in Personality*, Vol. 25, No. 3, 1991, pp. 285-301.
4. boyd,d.m., and Ellison, N.B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer Mediated Communication*, 13, 1, article 11, available at: http://jcmc.indiana.edu/vol13/issue1/biyd.ellison.html accessed December 11, 2008.
5. Carter, H.L., T. Foulger, and A. Ewbank. (2008) Have You Googled Your Teacher Lately? Teachers' Use of Social Networking Sites. Phi Delta Kappan, May, pp. 681-685.
6. Doll, Jork and Icek Ajzen. "Accessibility and Stability of Predictors in the Theory of Planned Behavior." *Journal of Personality and Social Psychology*. Vol. 63, No. 5, 1992, pp. 754-764.
7. Earle, T. and Cvetkovich G. (1995), *Social trust: Toward a Cosmopolitan Society*. Praeger, Westport, CT.
8. Felt, A. and D. Evans. (2008) Privacy protection for social networking APIs. *Web 2.0 Security & Privacy 2008 Workshop*, May 22, 2008, Oakland, CA, available at: http://www.cs.virginia.edu/felt/privacybyproxy.pdf, accessed December 15, 2008.
9. Foltz, C.B., Schwager, P.H., and Anderson, J.E. (2008) Why users (fail to) read computer usage policies, *Industrial Management & Data Systems*, 108, 6, pp. 701-712.
10. Goettke, R. and Christiana, J. (2007) "Privacy and Online Social Networking Websites." http://www.eecs.harvard.edu/cs199r/fp/RichJoe.pdf accessed December 15, 2008
11. Gross, R. and A. Acquisti. (2005) Information revelation and privacy in online social networks (The Facebook Case). (2005). *ACM Workshop on Privacy in the Electronic Society 2005*,. available at: http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf accessed December 15, 2008
12. Peluchette, J. and K. Karl. (2008) Social Networking Profiles: An Examination of Student Attitudes Regarding Use and Appropriateness of Content. CyberPsychology & Behavior, 11, 1, pp. 95-97.
13. Robert, P. H., Clairet, S., Benoit, M., Koutaich, J., Bertogliati, C., Tible, O., Caci, H., Borg, M., Brocker, P., and Bedoucha, P. (2002), "The apathy inventory: Assessment of apathy and awareness in Alzheimer's disease, Parkinson's disease and mild cognitive impairment", *International Journal of Geriatric Psychiatry*, Vol. 17 No. 12, pp. 1099-1105.
14. Singel, Ryan. (2009) Let's Learn From Facebook's Terms-of-Service Flap. Wired Blog Network. Available at http:/blog.wired.com/business/2009/02/facebook-flap.html. accessed February 19,2009.
15. Siegrist, M., Cvetkovich, G., and Roth, C. (2000), "Salient value similarity, social trust, and risk/benefit perception", *Risk Analysis*, Vol. 20 No. 3, pp. 353-362.
16. Skiba, D. (2008) "Nursing Education 2.0: Twitter & Tweets." Nursing Education Perspectives, 29, 2, pp. 110-112.