ONLINE SOCIAL NETWORKS AND THE PRIVACY PARADOX: A RESEARCH FRAMEWORK

Michael J. Mainier, Robert Morris University, mjmst3@mail.rmu.edu
Michelle O'Brien Louch, Robert Morris University, melst10@rmu.edu

ABSTRACT

There is a paradox of privacy within social networking sites such as Facebook and MySpace. Users join these sites for any number of reasons, from professional networking to keeping in touch with family and every reason in-between. Studies show that it is likely that users are not always as aware of privacy issues on the Internet, and probably share more information than they would if they were aware of their potential exploitation when their supposedly private data is accessed without permission. This paper will look the privacy issues that surround social networking sites and offer a research framework specifically focusing on the characteristics of an online social networker and the motivating factors that guide them as they communicate through a social networking website.

Keywords: Information Technology (IT), Social Networking, Ethics

INTRODUCTION

The Internet serves as a hub of digital communication utilized by businesses and universities worldwide in transacting information and services to consumers. A constant stream of text, images, audio, and video can be accessed at any time through computers and mobile devices within range of an Internet connection. This ability for users to remain continuously connected has pushed the innovation and advancement of the Internet to new heights allowing limitless consumption of news, entertainment, and communication between family and friends.

The emergence of the Internet has also flattened the world and brought about the development of new social trends. These trends are evident by the growing number of people interacting through virtual social networking websites such as Facebook, MySpace, Twitter, and LinkedIn [10]. By granting free registration to their members, each website provides a powerful online communication platform for sharing pictures, forming groups, and further interaction through multiplayer games. To give an example of how popular virtual social networks have become, *Facebook* reported 400 million subscribers as of April 2010 [4].

While the popularity of online social networking continues to grow so too does the increasing threat to member privacy. Member-posted content has the potential to be seen by millions of online viewers – regardless of the member's specific privacy expectations.

One of the primary reasons behind this accidental online exhibitionism is that members may not enable their privacy settings or be aware that someone is gaining access to their profile through an account they thought was a trusted friend. This is because many sites lack user-friendly settings and users are unable to determine if their pages are private or public [2]. For example, Livingstone's 2008 study [9] on social networking sites and teenagers, who are often stereotyped as being some of the most tech-savvy members of society today, revealed that many users did not know how to change their privacy settings. Often, users – regardless of age – simply fail to set their accounts to "private" because they do not know how or think that they already did. In essence, a poor understanding of privacy on the Internet in general means that not all users of a social networking site realize that it is public and thus lack the knowledge to protect themselves from unauthorized viewing [1].

As part of the privacy issue, there can be a sense of exclusive membership. Given the way that social networking sites require certain pieces of information from the users – asking for e-mail addresses, birth dates, and school affiliations – some users experience the illusion of privacy, as if they are joining an exclusive group [1]. Reinforcing this illusion is the fact that the advertisements on these sites are tailored to the user based on the data that he or she supplied during the registration phase [14]. According to Barnes [1], this illusion "creates boundry problems" that encourages users of social networking sites to post more information then may be prudent, including home addresses and phone numbers ". Reinforced by the fact that those who are online frequently access it from the "privacy" of their home, one may be prone to trust that the information shared is somehow shared only with whom the member wishes to share. Unauthorized access and use of private information found on a members social network profile can lead to countless dangers including; identity theft, fraud, stalking, and loss of employment [2].

As privacy concerns multiply, there is little evidence that social networks are losing members [2]. This phenomenon is known as the *privacy paradox* or, “the relationship between individuals' intentions to disclose personal information and their actual personal information disclosure behaviors” [11]. “For all the concern that people express about their personal information”, according to Norberg and co-researchers [11], “observations of actual marketplace behavior anecdotally suggest that people are less than selective and often cavalier in the protection of their own data profiles”.

RESEARCH RATIONALE

The objective of this paper is to present a research plan along with a rationale for exploring the *privacy paradox* in the context of online social networking member behavior. To further understand why people divulge private information in an online social network setting, four research questions are posed:

1. What are common characteristics do online social networkers share?
2. What are the motivating factors guiding online social networkers to communicate through a social networking website?
3. Among the information disclosed through a social networking website, what aspects do social networkers consider to be public or private?
4. What controls are they using to protect their private information?

This paper will explain the theoretical models employed to frame the study, introduce hypotheses that can be used to conduct future research, propose a methodology for data collection, and present expected findings. The major contribution of this research provides a framework in order to examine how knowledgeable online social networkers are regarding their privacy and the social factors driving their decision to post personal information online.

Theoretical Model and Hypotheses

This research plan will demonstrate use of two separate theories to frame and analyze each question. First, self-verification theory will be used to examine the motivating factors behind online social networking. Second, the theory of uncertainty avoidance will be used to analyze how online social networkers handle feelings of ambiguity in the context of controlling private information [7, 12].

The first two research questions focus on the basic characteristics of individuals who subscribe to websites like Facebook and MySpace and why they choose those outlets over other socializing activities. Technology and the Internet certainly make it easy and efficient to form personal bonds with others through use of text, audio, and other visual content such as images and video. However, further understanding is needed to explain the differences in individual behavior when disclosing personal information through an electronic social medium versus disclosing personal information in social interactions outside of the Internet.

According to self-verification theorists, individuals are constantly seeking out social situations that will verify their own self-conceptions [12]. The idea that people derive self-knowledge from engaging in social situations can be traced back to the theory of symbolic interactionism [13]. As Swann [13] notes, “After observing themselves repeatedly enact particular roles, the argument goes, people construct role-specific self conceptions”. Swann adds that this laid the foundation for the development of Erving Goffman’s dramaturgical frame which theorized that people take on the characteristics of actors on stage who assume a role [6, 13]. Swann adds [13], “Later scholars further expanded the formulation, emphasizing the tendency for people to maximize interpersonal harmony by gravitating toward social settings that seem likely to offer support for their identities or self-views”.

By applying the self-verification framework to the online social network setting, analyzing the motivating factors behind ones use of online social networks can be further analyzed. For example, a Facebook member can choose the images and information displayed on their profile which allows them complete control over how they might be perceived by other members in their network. After all, a “well-groomed” profile with information and images of their self perception may increase their acceptance into a network of friends and attract more visitors. Thus, it can be hypothesized (H1) that individuals feel they can control their own self-conceived role better in a virtual social network than they can while interacting in a more public setting offline.

However, does the need for socializing with others through virtual social networks outweigh the desire to safeguard personal privacy? The last two research questions focus on individual perception of private information and what factors alleviate concerns over the security of their private information. Avoiding this feeling of ambiguity can be analyzed through the theory of uncertainty avoidance. Uncertainty avoidance [7] is defined as "the extent to which the members of a culture feel threatened by ambiguous or unknown situations" and the desire for rules and regulations to avoid anxiety.

Members of these virtual social networks may feel a sense of security and control over all personal information because of privacy settings available to safeguard private information. According to the founder of Facebook, Mark Zuckerberg [3], "The problem Facebook is solving is this one paradox…People want access to all the information around them but they also want complete control over their own information". However, conflicting statements are found in Facebook's privacy policy [3] stating, "default privacy settings limit the information displayed in your public profile to your networks". Further reading garnishes a warning of "You post User Content…on the Site at your own risk…Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable". While no website is completely impenetrable from a virus or from those with less than honorable intentions, sites such as Facebook market themselves as trusted sites that help members control the information shared through privacy settings.

Therefore, to further explore the *privacy paradox,* a second hypothesis (H2) is that individuals who communicate through virtual social networks feel they have control over their own private information. Lastly, it is also thought (H3) that the majority of individuals who communicate through virtual social networks will confirm that they did not read the privacy policy before becoming a member.

SUGGESTED RESEARCH METHODOLOGY

Although no acceptable method of data collection could be found Data for this quantitative study will be collected through use of a questionnaire which will ask for responses in four different areas: member demographics, comfort level of communicating private information online vs. offline, personal account privacy setting patterns, and privacy policy awareness.

The population surveyed will consist of college students and recent graduates because most students have an active MySpace or Facebook account, a valid email account, access to a computer and Internet on a daily basis. The researcher will also have access to the university campus throughout the study. Because the study is not limited to college students, the questionnaire can also be distributed to any individual who has a valid email address, access to a computer and the internet.

Part I – Member Demographics

Member demographics will consist of collecting data on gender, age, race, marital status, computer usage, internet usage, where the member accesses the internet, how many virtual social networks in which they are members, and how often they log into their favorite social networking site. This information will provide an impetus for future research on the topic by demographic.

Part II – Communicating Online Vs. Offline

Users comfort level of communicating private information online vs. offline will be addressed by listing a series of personal events such as "getting married", "having a baby", "obtaining a new job" and using a five-point scale to determine their comfort level of communicating each piece of information in three social communication scenarios; face to face, virtual social networks, or other (telephone, email, letter). Comfort level refers to how willing someone is be to reveal this information, on a five-point Likert-type scale ranging from "Not comfortable" to "Very comfortable" [5]. For example, one may be very comfortable talking to someone face to face about having a baby, however, they may be not comfortable sharing this information across their virtual social network. Through analyzing individual comfort levels in different social contexts (offline vs. online), this survey will address the first hypothesis and shed light on how individuals control their own self-perceptions using different social mediums.

Part III – Patterns in Personal Privacy Settings

The second hypothesis can be addressed by gathering and examining patterns in personal account privacy settings. To assess these patterns, respondents can be asked to select the specific groups of people they allow to access certain characteristics of their virtual social network profile. For example, ten profile characteristics can be presented including; basic information (gender, birth date, relationship status), personal info (interest, activities, "about" the individual), status updates, phone number, home address, photos, photos and videos in which the member is tagged, education information, and employment information. Respondents can then select which groups they allow each characteristic to be revealed to. The choices for groups may include; friends, family, past-classmates, friends of your friends, anyone, information not revealed, cannot control, don't know, and not applicable. For instance, an individual may choose to only reveal photos to friends in their network and not family members. Or, they may not know if they have chosen to block past-classmates from viewing videos or images of themselves that others have posted (tagging). This survey question will assist in addressing how the uncertainty avoidance theory relates in the context of virtual social networks.

Part IV – Privacy Policy Awareness

The last area can consist of respondents answering three multiple choice questions regarding their awareness of privacy policies on virtual social network websites. The questions will include the following with corresponding choices below each question:

1. What is the most recent virtual social networking site you registered with?
   a. Facebook
   b. MySpace
   c. Twitter
   d. Other
2. Did you review the websites privacy policy before or after registering with your selection in question 1?
   a. Before
   b. After
   c. Did not review
3. If you answered " Did not review" in question 2, what would you state as your reason for not reviewing the websites privacy policy?
   a. I trust the website
   b. Couldn't find the privacy policy
   c. Didn't know about it
   d. No time
   e. Other.

EXPECTED RESULTS AND FURTHER RESEARCH

Through quantitative data gathering and analysis, the expected result of this study is to produce findings that will assist in furthering the awareness of privacy safeguarding across various virtual social network communities. The results may spark further interest by researchers to understand how privacy is being conceived in different groups outside of the United States. As virtual social networks continue to grow, perceptions of personal data privacy remain in discussion. A comprehensive literature review could consist of gathering records of current privacy laws and legal precedents awaiting judgment. The findings of this particular research framework are expected to reveal the need for further education of virtual social networkers concerning privacy safeguarding online.

REFERENCES

1. Barnes, S. B. (2006, September). *A privacy paradox: Social networking in the United States.* Retrieved May 16, 2009, from First Monday: http://firstmonday.org.
2. Brandenburg, C. (2008). *The Newest Way to Screen Job Applicants: A Social Networker's Nightmare*. Federal Communications Law Journal, 60(3), 597-626. Retrieved May 9, 2009, from ABI/INFORM Global database. (Document ID: 1536934351).
3. Facebook principles. (2008, November 26). Retrieved May 9, 2009, from Facebook Web site: http://www.facebook.com/policy.php
4. Facebook Press Room. (n.d.). Retrieved April 10, 2010, from Facebook Web site: http://www.facebook.com/press/info.php?statistics
5. Fink, A. (2009). *How to conduct surveys: A step-by-step guide*, 4th ed. Los Angeles: Sage Publications.
6. Goffman, E. (1974). *Frame analysis: An essay* on *the organization of experience.* Boston: Northeastern University Press.
7. Hofstede, G. & Hofstede, G. J. (2005). *Cultures and organizations.* New York: McGraw-Hill.
8. Howard, B. (2008). *Analyzing Online Social Networks*. Communications of the ACM, 51(11), 14-16. Retrieved May 9, 2009, from 7. Business Source Premier database.
9. 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*, 393-411.

10. Lucky, R. (2008). Zero Privacy. IEEE Spectrum, 45(7), 20. Retrieved May 9, 2009, from ABI/INFORM Global database. (Document ID: 1511346521).
11. Norberg, P., Horne, D. R., Horne, D. A. (2007). *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors.* The Journal of Consumer Affairs, 41(1), 100-126. Retrieved May 9, 2009, from ABI/INFORM Global database. (Document ID: 1435096751).
12. Swann, W. B., Jr., Stein-Seroussi, A., & Giesler, B. (1992). *Why people self-verify*. Journal of Personality and Social Psychology, *62*, 392-401.
13. Swann, W.B., Jr., Johnson, R.E., & Bosson, J. (2009). *Identity negotiation in the workplace*. In B. Staw & A. Brief (Eds.), Research in organizational behavior. Amsterdam, The Netherlands: Elsevier.
14. van Wel, L. & Royakkers, L. (2004). Ethical issues and data mining. *Ethics and Information Technology 6*, 129-140.