8-1-2008

Perceptions of privacy on Facebook

Elizabeth A. Warfel

Running head: PERCEPTIONS OF PRIVACY

The Rochester Institute of Technology

Department of Communication

College of Liberal Arts

Perceptions of Privacy on Facebook

by

Elizabeth A. Warfel

A Paper submitted

in partial fulfillment of the Master of Science degree

in Communication & Media Technologies

Degree Awarded:

August 11, 2008

The following members of the thesis committee approve the thesis of Elizabeth A. Warfel on August 11, 2008

Bruce A. Austin

Bruce A. Austin, Ph.D.
Chairman and Professor of Communication
Department of Communication
Thesis Adviser

Rudy Pugliese

Rudy Pugliese, Ph.D.
Professor of Communication
Coordinator, Communication & Media Technologies Graduate Degree Program
Department of Communication

Deborah Blizzard

Deborah Blizzard, Ph.D.
Assistant Professor
Department of Science, Technology and Society/ Public Policy
Thesis Adviser

Thesis/Dissertation Author Permission Statement

Title of thesis or dissertation: ***Perceptions of Privacy on Facebook***

Name of author: Elizabeth A. Warfel
Degree: Master of Science
Program: Communication & Media Technologies
College: College of Liberal Arts

I understand that I must submit a print copy of my thesis or dissertation to the RIT Archives, per current RIT guidelines for the completion of my degree. I hereby grant to the Rochester Institute of Technology and its agents the non-exclusive license to archive and make accessible my thesis or dissertation in whole or in part in all forms of media in perpetuity. I retain all other ownership rights to the copyright of the thesis or dissertation. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

Print Reproduction Permission Granted:

I, __Elizabeth A. Warfel_____, hereby **grant permission** to the Rochester Institute of Technology to reproduce my print thesis or dissertation in whole or in part. Any reproduction will not be for commercial use or profit.

Signature of Author: ___Elizabeth A. Warfel_____ Date: __August 11, 2008_____

Print Reproduction Permission Denied:

I, _____, hereby **deny permission** to the RIT Library of the Rochester Institute of Technology to reproduce my print thesis or dissertation in whole or in part.

Signature of Author: _____ Date: _____

Inclusion in the RIT Digital Media Library Electronic Thesis & Dissertation (ETD) Archive

I, ____Elizabeth A. Warfel _, additionally grant to the Rochester Institute of Technology Digital Media Library (RIT DML) the non-exclusive license to archive and provide electronic access to my thesis or dissertation in whole or in part in all forms of media in perpetuity. I understand that my work, in addition to its bibliographic record and abstract, will be available to the world-wide community of scholars and researchers through the RIT DML. I retain all other ownership rights to the copyright of the thesis or dissertation. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation. I am aware that the Rochester Institute of Technology does not require registration of copyright for ETDs. I hereby certify that, if appropriate, I have obtained and attached written permission statements from the owners of each third party copyrighted matter to be included in my thesis or dissertation. I certify that the version I submitted is the same as that approved by my committee.

Signature of Author: _____Elizabeth A. Warfel_____ Date: ___August 11, 2008__

Table of Contents

PERCEPTIONS OF PRIVACY ON FACEBOOK

Name: Elizabeth A. Warfel
Department: Communication
College: Liberal Arts
Degree: Master of Science in Communication & Media Technologies
Term Degree Awarded: Summer 2008 (20084)

Abstract

Information privacy in an information age is a paradoxical issue, especially with the recent innovations of the Internet. Social networking sites collect a great deal of personal information about their users. Previous studies regarding both traditional and online commercial marketplace privacy issues have found consumers to be wary of disclosing personal information, but also unaware of the regulations concerning sharing of customer information among companies. This study focused on the differences between heavy and light users' perceptions on privacy on Facebook. Results from a 25-question survey showed heavy users of social networking sites perceive a greater depth of communication on Facebook and have a more accurate perception of Facebook's privacy policy than did light users of social networking sites.

Keywords: Privacy, Privacy Policy, Online Privacy, Social Networking Sites, Facebook

Would you give your name and phone number to a complete stranger? Maybe. What about your age, picture, email, birthday, and billing address? It is possible you already have done so. Every day people compromise their privacy online. Although some research show Americans as cautious and wary when disclosing information on the Internet (Turow & Hennessy, 2007), other arguments (Barnes, 2006) suggest that people may not realize what they have given away or how accessible their information really is.

When discussing privacy and the Internet, a number of studies have focused on privacy in regards to online marketing and making online purchases (Markel, 2005; Sheehan & Hoy, 2000; Turow & Hennessy, 2007; Turow, Hennessy & Bleakley, 2007). These studies have found consumers to be both trusting and suspicious when revealing personal information to an online entity. Shopping online, however, is not the only way consumers disclose personal information on the Internet. Social networking sites (SNS) also collect a great deal of personal information about their members.

As social networking sites become more and more popular, they may be one place on the Internet where users feel more secure than they actually are.[1] Facebook alone has 58 million active users (Rosenbloom, 2007, para. 6) all of who have handed over some personal information to be a part of the site. Many people view social networking sites like Facebook and MySpace as private webpages and are willing to display personal information such as their name, address, and other contact information. Users may also post personal photos, blogs and links. Because the users view their pages as private, they would not expect the information posted to be viewed by the general public.

[1] Why do social networking sites seem a safe place on the Internet? It might be speculated that people associate social situations with safety and trust, while business and transactional situations are associated with an absence of safety and trust.

The users' possible misperceptions about privacy could affect them in unforeseen ways. Barnes (2006) suggests schools use social networking sites to monitor their students' behavior, and increasingly college students are warned that their Facebook or MySpace page may be perused by prospective employers. So why do students continue to display private information in a public sphere?[2] People may expect a level of privacy from Facebook and MySpace that isn't realistic. Or, they may trust the online community and believe that its privacy policy protects their information from marketers, strangers and prying eyes. Another possibility is that people do not read or know what they are agreeing to when they acknowledge they have "read" the privacy policy.

When a person signs up on a site such as Facebook, she must accept the privacy policy to join the network. The privacy policy states her personal information can be disclosed for advertising and marketing purposes, and will be turned over to the police when necessary (Hodge, 2006; Facebook Privacy Policy, 2007). And millions have joined the SNS, giving up their private information for the use by the site.

The question of privacy, specifically on social networking sites, has led to the present investigation of the differences in self-reported perceptions and expectations of privacy between heavy and light users of social networking sites. The three research questions this study explored were: (1) What differences are there between self-reported heavy and light users of social networking sites and the user's self-reported perceived depth of communication? (2) What

[2] In regards to a public sphere, how has digital media changed what is understood to be a public space? As an online social community, it might be assumed that the shared space is public. However, users may view their webpages as similar to a home where only those invited in can see what is displayed. Of course, the major difference is that a home is not crawling with electronic spiders gathering information on the home dweller's preferences, navigation and displayed information so as to better market to her. There is also nothing in one's home that patrols through photo albums looking for incriminating pictures of underage drinking.

differences are there between self-reported heavy and light users of social networking sites and their self-reported perceived levels of privacy? (3) What differences are there between self-reported heavy and light users of social networking sites and their self-reported desired levels of privacy? By answering these questions we can better determine expectations and desire for communication privacy, how well members know Facebook's privacy policy and how they view their own communication via the social networking site.

The first research question tries to determine whether users consider their communication personal or public. It could be argued that personal communication would have a higher expectation of or desire for privacy whereas public communication could be argued to require little privacy and fall into a public sphere. These questions will also determine whether users have read Facebook's privacy policy and have an accurate perception of the policy (question 2), and what level of protection they wish they had over their information (question 3).

Thus far, researchers of digital social networking sites have studied the interaction and interpersonal relationships that are being digitally recorded on personal webpages. Much of the past discussion regarding social networking sites and privacy has revolved around safety for teenagers and safeguarding personal identity (Barnes, 2006; Boyd & Ellison, 2007). In these studies privacy has often been viewed as a way to protect minors from predators. However, the crucial question of whether social networking sites' users view their own digital communication as a public or private endeavor remains to be explored.

Depth of communication refers to how personal the user views his or her communication with others. There are two reasons for establishing the user's perception of their depth of communication. First, if the communication is considered highly personal, then the participants

would most likely expect a higher level of privacy and have a higher level of trust in Facebook not to expose their personal information. An expectation of privacy on Facebook could legally protect the medium under the Fourth Amendment. This may give Facebook users' grounds for legal redress if their privacy is invaded. This could be very significant for the millions of Facebook users.

Second, if the space is established to be private, then ethically researchers should not observe the online communication without the participants' knowledge. However, if the space is considered public, the online communication is publicly observable.[3] Gaining knowledge of users' perceptions of online social networking space as public or private will indicate how researchers should proceed to do research on online social networking sites.

Barnes (2006) found that respondents were generally neutral in their responses to the statement, "Facebook respects my privacy." Her study also points out, however, that many users are not aware of their lack of privacy on the Internet. The awareness issue is what has motivated me to do this study. My casual observation is that many users of social networking sites have no idea what Facebook's policy does not protect. The users perceive their webpages as personal and private, and thus reveal information they would not in a public domain. Further research may determine if Facebook users perceive the online social networks as private spaces and therefore expect protection of privacy, even though the site may clearly state in its privacy policy that it will not provide it.

Review of Related Literature

[3] This question could, of course, be expanded to ask, do we have human subjects on the Internet? Are we even observing people, or just people's behavior online? Is there a difference between studying a person and a behavior?

In a study of YouTube, a video social networking site, Lange (2007) concluded that privacy online can no longer be classified as strictly public or private. The study examined the "fractalized patterns" (para. 14) of communication through interviews, observations and analyses of posted videos and comments, and examination of subscription and friending practices on YouTube over the course of a year. Lange reported a dichotomy of publicly private and privately public behavior. The dichotomy refers to the idea that the user's identity may be public or private, and the user's page content may be public or private. Lange found the user's identity and the user's content to be two separate items in regards to privacy. Her term "publicly private behavior" is when the YouTube creator's identity is public, but the video content is only available to those people the creator chooses thereby making the content private. "Privately public behavior" is when the video's creator's identity is kept private (i.e. anonymous or the creator uses an alias), but the video content is publicly accessible. If applying this concept to social networking sites, users may choose to take on either publicly private or privately public behavior by disguising their real names, restricting accessibility to their webpages or selectively limiting what they display on their webpages.

Privacy is a very complex and contextual issue. From previous research and their own, Sheehan and Hoy (2000) suggest five factors that influence the level of concern an online consumer feels when divulging private information: Awareness of the information being collected, how the information will be used, the information's sensitivity, how familiar the consumer is with the entity collecting the information, and what the consumer is receiving in exchange for their personal information. All of these factors, plus the user's relationship with the entity collecting the information, may come into play when a user decides to reveal personal

information on a social networking site. Sheehan and Hoy's study consisted of an email survey completed by 889 people who were chosen randomly from the *Four11 Directory Service*. The results indicated that consumers were less concerned with their privacy when they were aware the online business was collecting it, and when they felt they were in control of how the information would be used. Also, the more the person trusted the entity collecting the information, and the greater the compensation for providing information, the more likely the individual was to disclose personal information. Applying this research to a social networking site is useful. Sheehan and Hoy's study would suggest that Facebook's users would feel more comfortable disclosing information if they trust Facebook to guard their information, if they felt they were getting a reward (such as free use of the service), and if the users felt they were in control of how their information would be used. It also suggests awareness of the kind of information being collected will play a major role in how comfortable Facebook users are in sharing their personal information.

Turow, Hennessy and Bleakley (2007) studied Americans' understanding of commercial privacy regulations. They were interested in discovering the general "schemata or cognitive structure" (p.4) people have about companies' ability to collect their personal information online. They also explored how knowledgeable people were in regard to information sharing regulations between companies. Their research found that many Americans were very concerned about privacy on the Internet, but knew very little about the actual policies concerning private-information sharing between online merchants. While the study's respondents had a vague knowledge of information-sharing practices, they were very inaccurate in knowing the process and rules that govern organizations that hold their data. Like Markel (2005) and Baruh (2007),

Turow, Hennessy and Bleakley suggest a clear national outline of marketplace privacy rights may need to come from the government in order to better inform, educate and protect online consumers.

In the United States, privacy is an "indispensable component of security" (Markel, 2005, p. 202), and Markel argues the individual's right to control access to personal information is an intrinsic good—something that benefits all in society. The creators of the Constitution were well aware of privacy's importance, protecting "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…" (U.S. Constitution, Amendment IV). In 1967, through the decision in *Katz vs. United States*, the literal interpretation of the Fourth Amendment was expanded by deciding that the protection of people and not property was the Fourth Amendment's purpose (Hodge, 2006). But neither of these legal landmarks was established in an age of the Internet. In the new information age, there is not a comprehensive law that protects "individuals' informational privacy rights in the USA" (Baruh, 2007, p. 198). Instead, Congress relies on past cases with comparisons between old media and the new medium in question (Baruh, 2007; Hodge, 2006). In the U.S., commercial websites have set up privacy policies and adhere to self-regulation in an attempt to avoid government regulation. Groups such as The Direct Marketing Association, the Association for Internet Marketers and the Internet Advertising Bureau are some of many organizations that have taken on the task of creating privacy models for an online economy (Turow & Hennessy, 2007). So far, the U.S. has decided not to regulate online businesses privacy policies, despite the fact that other countries (Canada and those in the European Union) have decided to do so (Markel, 2005).The U.S. may have taken this hands-off approach based on the ideals of a free marketplace—leaving

it up to the population to decide what should be private based on what consumers are willing to hand over. With a subject as complex and contextual as privacy, SNS users may be the only ones who can determine this for social networking sites.

Perhaps because of the lack of government policy, cyberspace privacy is emerging as a legal question, in particular, with regards to online communication and social networking sites. As Boyd and Ellison write (2007, para. 53), SNS are "challenging the legal conceptions of privacy." The example they give is the question of whether a police officer can search the information posted on a site such as Facebook without a warrant. Hodge (2006) explored the same question and determined that the legal right to privacy depends on whether the community of users expects a level of privacy on the site. If the users can prove that they do not intend their disclosed information to be made public, then it would be reasonable to conclude social networking is a private form of communication. Parallels could be drawn between SNS and the telephone. It is important to remember that telephones were not always a private medium. The earliest telephone lines were party lines where there really wasn't a reasonable expectation of privacy because anyone on the line could listen in. The user of the telephone weighed the benefits of using the phone against the risks of someone listening-in on their conversation just as SNS users weigh the benefits of using the site with the risks of handing over private information. Today, with the innovation of private telephone lines, the user's expectation of privacy has changed to a reasonable one. The telephone company, as the provider of the medium, collects information on both the caller and the receiver, but is not responsible for, nor privy to, the content that is communicated over the communication device (Hodge, 2006). It is, therefore, the evolution of technology that changes the user's reasonable expectations of privacy.

"Information about individuals' media consumption habits make up an increasingly large share of the stock of data that institutions compile about individuals" (Baruh, 2007, p. 188). According to Hodge (2006), the best way users can demonstrate the intent to keep their information private is by applying the privacy settings on their Facebook or MySpace pages. He calls these "limited profiles" as they grant limited access to viewers. According to Lange (2007), this would be a publicly private profile. He states default profiles (profiles where the user does not apply privacy settings beyond the default settings of the application) would most likely fall under the plain view doctrine. Therefore, according to Hodge, only limited profiles in which the user has acted to keep her information private could be protected under the Fourth Amendment.

Even limited profiles, however, are created and stored on a remote server owned by the social networking site. This poses another question in the privacy debate. The Supreme Court has previously ruled that by disclosing information to a third party, the person gives up her expectation of privacy (Hodge, 2006). However, again, this traditional approach may not be adequate for an online policy. The users' expectations of privacy need to be considered by Facebook administrators, the government and researchers because an expectation of privacy may shape a user's behavior on a social networking site. If the user expects the third party to protect her privacy, the information would fall under the Fourth Amendment. Also, if the user does not see the administrators as the intended recipient of the information, the expectation of privacy can be upheld based on the third party being a necessary medium to communicate with the intended recipient (Hodge, 2006). It is the researcher's observation that most SNS users rarely consider the administrators of the site they are using.

The previous literature seems to designate much of the accountability for privacy to the social networking site user. Lange (2007), Sheehan and Hoy (2000), and Turow, Hennessy and Bleakley (2007) all mention the user's responsibility to know his or her privacy rights and educate him- or herself on different privacy options. Hodge (2006) points out that an expectation for privacy may be enough to grant privacy, but only if the user demonstrates that expectation.

Method

The three research questions this study explored are: (1) What differences are there between self-reported heavy and light users of social networking sites and the user's self-reported perceived depth of communication (highly personal vs. superficial)? (2) What differences are there between self-reported heavy and light users of social networking sites and their self-reported perceived levels of privacy? (3) What differences are there between self-reported heavy and light users of social networking sites and their self-reported desired levels of privacy?

To address the research questions, a survey was conducted using the Rochester Institute of Technology's (RIT) email network. A pre-test of the survey instrument was conducted using 10 Facebook users who were not members of the RIT email network. By choosing pre-test respondents outside of RIT's email network, it assured no respondent saw the survey twice. The pre-test allowed the researcher to establish if there were any problems understanding any of the questions on the survey instrument. It also let the researcher estimate the time it would take for respondents to complete the survey.

The survey was distributed through RIT's email network via an email that gave recipients a short explanation of the intended research, the estimated time needed to complete the survey, a

link for recipients to click on to take the survey, and contact information for the researcher (see Appendix B). Motivation to complete the survey was given in the form of a social rationale—in filling out the social networking site privacy survey, the recipient was able to voice his or her opinion and concerns on what is and what should be considered private in regards to social networking. The link took the respondent to a survey host site. The survey host site, clipboard.com, assured only one survey was taken from each IP address and login name. Although this does not technically make it impossible for the same person to submit the survey twice (those people who are technically savvy enough to hack clipboard could take the survey twice), it does make it substantially more difficult for a person to do so.

By distributing the survey through Rochester Institute of Technology's email network, respondents were able to complete the survey online with minimal click-through effort. It also insured respondents were of a mature age. This is important since Facebook's privacy policy does not allow anyone under the age of 13 to have a Facebook webpage, and suggests children between the ages of 13 and 18 ask their parents for permission before using the site.

The variables this survey operationalized are self-reported levels of use of social networking sites, self-perceived depth of conversation, perceived levels of privacy based on knowledge of Facebook's privacy policy, and desired levels of privacy. A respondent's level of use was determined through a closed-ended behavior question with ordered answer choices on a four point scale. Each answer choice indicated the numbers of hours spent on social networking sites in the past 24 hours. The past 24 hours was chosen as the time frame to reduce self-reporting error. It was determined after all survey responses were collected that light users were

users who spent less than one hour of a social networking site while heavy users were anyone who spent one or more hours on social networking sites. This operationalized the first variable.

Self-perceived depth of communication was measured through a set of five belief statements aimed at establishing how the respondents viewed their own communication on Facebook. The respondents were given four closed-ended ordered answers on a four point scale: strongly agree, agree, disagree, or strongly disagree. The respondents were asked to choose only one answer per question. A four point scale was chosen to avoid having a neutral position. Together, the respondent's answers to the five belief statements were coded to assess his or her self-perceived depth of conversation. Each answer was assigned a number value. If the answer indicated a high level of personal communication, it was assigned a one (1). An indication of a low level of personal communication was assigned a four (4). The respondent's answers to the five belief statements were then added together to give each respondent a total score for self-perceived depth of communication. To view the number value assigned to each answer, please see Appendix B.

Perceived level of privacy was determined through 10 statements in which the respondents could answer True or False. These statements were created from Facebook's privacy policy to "test" how knowledgeable the users are on their privacy rights. The idea of testing users' knowledge of their privacy rights was taken from a previous study (Turow, Hennessy, & Bleakley 2007). These questions gave the researcher insight into what Facebook users think their level of privacy is when using the site. Every question that is answered correctly was assigned a value of two (2), every question answered incorrectly was assigned a value of one (1). A total was then added up for each respondent in this section. The higher the respondent's total, the

more accurate her perception of privacy is. This section of the survey answered the second research question.

Desired levels of privacy were determined through a series of four belief statements with closed-ended ordered answers on a four point scale: strongly agree, agree, disagree, or strongly disagree. The idea of using belief statements was taken from a previous study (Barnes, 2006). A four point scale was chosen so as to avoid having a neutral position. The respondents were instructed to choose only one answer for each question. The first two of these questions pertain to marketing and allowing Facebook, as a third party, the ability to search the content of a personal webpage. Marketing to users on their own webpages could be viewed as an invasion of privacy. Each answer was assigned a number value. If the answer indicated a low level of privacy concern, it was assigned a one (1). An answer indicating a high level of privacy concern was assigned a four (4). To view the number value assigned to each answer, please see Appendix B. The third question asked the respondents about having their information searchable in general in an effort to test at what point the respondent does not feel comfortable having their page searched. The same value scale was assigned to the third question as the previous two. The fourth question indirectly asks if Facebook's privacy policy is protective enough with the statement "When it comes to my privacy, Facebook is very protective." An answer of "Strongly Agree" or "Agree" indicated an adequate level of protection felt by the user and was assigned a one (1) and two (2) respectively, while an answer of "Disagree" or "Strongly Disagree" indicated a desire for higher levels of privacy and was assigned a three (3) and a four (4), respectively. To view the complete survey, please see Appendix B.

Lastly, demographic information was collected about the respondents at the end of the survey in order to describe the sample and compare heavy and light users. This information is collected in Part V of the survey.

Results

The survey was completed by 84 participants. The majority of the respondents were female (66%), and 73% of the respondents fell into the 18 to 23 age range while 16% of the respondents were in the 24 to 29 age range. Roughly 53% of respondents were undergraduate students, 25% were graduate students, 11% were alumni, 7% faculty, and 4% were staff. The majority of the respondents identified themselves as Caucasian (81%). Of the respondents, 67% were designated light users because they spent less than one hour on social networking sites in the last 24 hours. Heavy users were represented by 33% of respondents. Heavy users had spent an hour or more on social networking sites in the last 24 hours.

To answer the first research question, a t-test compared heavy and light users and their total perceived depth of communication. Results showed that heavy users perceived a significantly ($t = 2.387$, $df = 82$, $p = .019$) greater depth of communication than light users.

The second research question asked, what are the differences between heavy and light users of social networking sites and their perceived levels of privacy? To answer this question a t-test was run between heavy and light users and the total scores for perception of privacy. Results showed that heavy users had a significantly ($t = -2.250$, $df = 82$, $p = .027$) more accurate perception of Facebook's privacy policy than light users.

The third research question looked for the difference between heavy and light users of social networking sites and their desired levels of privacy. Again, a t-test was used to analyze the

results and there was no significant difference between heavy and light users and their desired level of privacy.

Lastly, no significant difference was found between heavy and light users and age or gender. Neither characteristic made a user more prone to fall into the heavy or light user category.

Discussion

With such a small sample these results are not conclusive. However, the two significant findings can be placed logically within the previous research. Perhaps heavy users are in fact heavy users of online social networking sites because the site provides them with a greater perceived depth of communication. With a greater perceived depth of communication, users are getting more from the site and therefore find it worthwhile to spend time online to keep up-to-date with others who also use the site. The previous research conducted by Sheehan and Hoy (2000) suggested many factors that influence the level of concern an online consumer feels when divulging private information. One factor was what the consumer perceived they were receiving in exchange for their personal information. The current finding suggests that heavy users find communicating online more important than light users. In return for use of the site, heavy users are willing to hand over personal information because the risks are outweighed by the benefits they receive when communicating on social networking sites.

It also could be argued that people who spend more time online use some of that time to read the privacy policies and therefore have a more accurate perception of Facebook's privacy policy. Heavy users of social networking sites might use some of their online time to surf around social networking sites, and in surfing, are more likely to find and read the site's privacy policy.

However, Sheehan and Hoy's (2000) research is also applicable here because they found consumers were less concerned with their privacy when they were aware the online business was collecting it, and when they felt they were in control of how the information would be used. Therefore, heavy users of social networking sites may also be heavy users having read the privacy policy online and thereby feeling more comfortable using the site because they are aware of how Facebook collects information and for what purpose. The user may also feel more in control of his or her information when he or she learns how to change default settings and opt-out of certain marketing services.

It was surprising to find no conclusive connection between age and gender and social networking site use. This could again be because of the homogenous sample population as well as the small number of responses.

Conclusion

Online privacy is a complicated subject. Research has often focused on how people understand their privacy rights when completing transactions online. Social concern for privacy policies with online merchants should not ignore the fact that many people give away their personal information when conducting online social transactions. This research studied users of Facebook and how they understand their privacy rights when using the social networking site.

Inherent limitations of the study include self-reported data. Since the study aims to measure attitudes towards privacy on social networking sites, it must rely on what the respondents say their beliefs are. Also, conducting the survey only through the RIT's email network limits the results. The results will only show what students, faculty, staff and alumni using an RIT email address who are also active users of Facebook perceive and desire their level

of privacy to be on social networking sites. As a technological school, RIT students may be more adept at navigating the online world of Facebook and inherently be more aware of the privacy policy. Conversely, RIT students may also be more trusting of technology because they feel more comfortable using it.

These results cannot be applied to all users of social networking sites, nor can they be applied to any social networking sites other than Facebook. Also, as Sheehan and Hoy (2000) point out in their own research, people concerned with privacy are less likely to actually take a survey. Consequently, those with the most extreme privacy concerns may not be represented by the sample.

Future research possibilities are abundant in this area. A study could seek to measure the compensation users perceive they receive when giving away their personal information. Users are not allowed to participate in the site unless they agree to Facebook's privacy policy which states that Facebook may give their information to third parties for marketing purposes. An interesting study would find at what point users become uncomfortable enough with the privacy practices of the site to opt-out of using the site altogether. Or, are there some users (a heavy user with a great depth of communication score for example) who would never opt-out of the site no matter how much information he or she had to disclose?

A similar study to this one could be expanded to social networking sites other than Facebook such as MySpace and LinkedIn. Knowledge of privacy policies could be compared between the different social networking site's users. It would be interesting to focus on users who use multiple sites. It also would be informative to compare the privacy policies of these sites

and see which one protects users the most. Of course, this exact study could also be expanded to a greater population which would provide more conclusive results.

References

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9). Retrieved January 11, 2008 from http://www.firstmonday.org/issues/issue11_9/barnes/index.html

Baruh, L. (2007, April 2). Read at your own risk: Shrinkage of privacy and interactive media. *New Media and Society*, 9, 187-211.

Boyd, D.M., & Ellison, N.B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), article 11. Retrieved January 11, 2008 from http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

Facebook Privacy Policy. Last accessed February 14, 2008 from http://rit.facebook.com/policy.php

Hodge, M.J. (2006). The Fourth Amendment and privacy issues on the "new" Internet: Facebook.com and MySpace.com. *Southern Illinois University Law Journal*, 31, 95-122. Retrieved January 21, 2008 from http://vnweb.hwwilsonweb.com.ezproxy.rit.edu/hww/Journals/getIssues.jhtml?sid=HWW:OMNIFT&issn=0145-3432

Lange, P.G. (2007). Publicly private and privately public: Social networking on YouTube. *Journal of Computer-Mediated Communication*, 13(1), article 18. Retrieved January 11, 2008 from http://jcmc.indiana.edu/vol13/issue1/lange.html

Markel, M. (2005). The rhetoric of misdirection in corporate privacy-policy statements. *Technical Communication Quarterly*, 14(2), 197-214. Retrieved February 7, 2008 from Communication & Mass Media Complete.

Reinard, J.C. (2008). *Introduction to communication research*. New York: The McGraw-Hill Companies, Inc.

Rosenbloom, S. (2007, December 17). On Facebook, scholars link up with data. *The New York Times*. Retrieved December 17, 2007 from http://www.nytimes.com/2007/12/17/style/17facebook.html?pagewanted=print

Sheehan, K.B. & Hoy, M.G. (2000, Spring). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19(1), 62-73. Retrieved January 17, 2008 from Communication & Mass Media Complete.

Turow, J. & Hennessy, M. (2007). Internet privacy and institutional trust: insights from a

national survey. *New Media & Society*, 9, 300-318. Retrieved January 23, 2008 from nms.sagepub.com.

Turow, J., Hennessy, M., & Bleakley, A. (2007). *How do Americans understand marketplace privacy? Findings from a national survey*. *Conference Papers—International Communication Association; 2007 Annual Meeting* (pp. 1-22). Retrieved January 30, 2008 from Communication & Mass Media Complete.

Appendix A: Sources Searched

www.nytimes.com

- 1981–present
- Searched:
    - Facebook

Journal of Computer-Mediated Communication

- 1995–December, 2007
- Searched:
    - Facebook
    - Social Networking Sites

ComAbstracts

- 1966–Present
- Searched:
    - Facebook
    - Privacy
    - internet privacy
    - public information and the Internet
    - perceptions of privacy
    - social networking privacy
    - social networking
    - online social networks
    - public versus private

  - research guidelines

Communication & Mass Media Complete

- Archive dates based on each publication
- Searched:
  - private versus public
  - facebook
  - privacy on the Internet
  - perceptions of privacy
  - privacy
  - privacy and expectation
  - privacy studies
  - studies in privacy
  - privacy and fear
  - privacy and knowledge
  - Sandra Petronio and Communication Privacy Management Theory

Appendix B: Survey Instrument

"Cover Letter" with Link to Survey

Dear Students, Faculty and Staff,

As I'm sure you are well-aware, safety and security on the Internet is a constant concern. You have been selected to participate in an important but voluntary research survey reflecting that concern. This survey will demonstrate what users of Facebook know and feel in regards to their privacy when using the social networking site. You must be a current user of Facebook to participate in this study. The collected data will remain anonymous, and the survey will take you no more than five minutes to complete. Your input is essential to create an accurate assessment of Facebook's privacy policy—something that may benefit future and current Facebook users—but you may also choose not to participate in the survey at any point by simply closing your browser's window. To take the survey, please click http://clipboard.rit.edu/takeSurvey.cfm?id=5ew6cx to be directed to clipboard, RIT's secure survey site. The survey will be available until 11 p.m. Wednesday, July 2. It is not anticipated this survey will pose any risks to survey participants, however, if you have any questions, please do not hesitate to email me at eaw4994@rit.edu. Your participation is appreciated!

Elizabeth Warfel

RIT Candidate for Master's in Communication and Media Technology

Survey Instrument

Thank you for agreeing to participate in this study! The survey has four sections, and a total of 25 questions. Pre-tests show it takes less than five minutes to complete the entire survey. Your input will help establish an accurate perception of Facebook's Privacy Policy!

Part I of V
Please choose one circle to answer the following question.

1. In the past 24 hours, how much time have you spent online on Facebook, MySpace, LinkedIn, or similar social networking sites?
   a. Less than 1 hour
   b. 1 to 2 hours
   c. A little more than 2 to 3 hours
   d. More than 3 hours

Part II of V
Below are five statements about Facebook. 1 indicates you strongly agree and 4 indicates you strongly disagree. Please show how much or how little you agree with each statement by clicking on one circle.

1. The conversations that take place on Facebook mean a lot to me.
   a. Strongly Agree (assigned value of 1)
   b. Agree (assigned value of 2)
   c. Disagree (assigned value of 3)
   d. Strongly disagree (assigned value of 4)

2. The conversations that take place on Facebook shape my friendships.
   a. Strongly Agree (assigned value of 1)
   b. Agree (assigned value of 2)
   c. Disagree (assigned value of 3)
   d. Strongly Disagree (assigned value of 4)

3. Leaving a message on a friend's "wall" is like waving at them at the mall.
   a. Strongly Agree (assigned value of 4)
   b. Agree (assigned value of 3)
   c. Disagree (assigned value of 2)
   d. Strongly Disagree (assigned value of 1)

4. I think of Facebook as a private communication tool, much like calling someone on the phone.
   a. Strongly Agree (assigned value of 1)
   b. Agree (assigned value of 2)
   c. Disagree (assigned value of 3)
   d. Strongly Disagree (assigned value of 4)

5. I like to use Facebook to see what a lot of different people are up to in a short amount of time.
   a. Strongly Agree (assigned value of 4)
   b. Agree (assigned value of 3)
   c. Disagree (assigned value of 2)
   d. Strongly Disagree (assigned value of 1)

Part III of V
Next we present you with a series of statements. For each one, please indicate whether you believe the statement is true or false by clicking on the appropriate circle.

1. Facebook is allowed to collect information on me such as my name, email, home address, IP address, telephone number and gender. (TRUE—2) (FALSE—1)

2. Facebook allows me to accept default privacy settings or to set my own. (TRUE—2) (FALSE—1)

3. Facebook is not allowed to keep track of people or groups I search but do not join. (FALSE—2) (TRUE—1)

4. I know where to find Facebook's privacy policy. (TRUE—2) (FALSE—1)

5. I have read Facebook's privacy policy. (TRUE—2) (FALSE—1)

6. Facebook guarantees that information I post as "private" will not be viewed by people other than those to whom I give permission. (FALSE—2) (TRUE—1)

7. Facebook is allowed to track my name through newspapers, blogs, instant message, or other user's pages. (TRUE—2) (FALSE—1)

8. Facebook allows Google search engine "crawlers" to access my name and picture on Facebook. (TRUE—2) (FALSE—1)

9. Applications developed by a Platform Developer outside of Facebook still must abide by Facebook's privacy policy. (FALSE—2) (TRUE—1)

10. I know how to opt-out of Facebook's Beacon Service. (TRUE—2) (FALSE—1)

Part IV of V
You're almost done! For the next four questions, please indicate how much you agree or disagree with each statement. 1 indicates you strongly agree and 4 indicated you strongly disagree. Please choose only one answer for each question.

1. Facebook should be able to use my name and email address to market certain services to me.
    a. Strongly Agree (assigned value of 1)
    b. Agree (assigned value of 2)
    c. Disagree (assigned value of 3)
    d. Strongly Disagree (assigned value of 4)

2. It's not ideal, but I'd rather have Facebook place marketing content on my page than have to pay to use Facebook.
   a. Strongly Agree (assigned value of 1)
   b. Agree (assigned value of 2)
   c. Disagree (assigned value of 3)
   d. Strongly Disagree (assigned value of 4)

3. I think the content of my webpage—what I write on my friends' walls and the pictures I post, for example—is private and should not be searchable by Facebook or anyone else.
   a. Strongly Agree (assigned value of 4)
   b. Agree (assigned value of 3)
   c. Disagree (assigned value of 2)
   d. Strongly Disagree (assigned value of 1)

4. When it comes to my privacy, Facebook is very protective.
   a. Strongly Agree (assigned value of 1)
   b. Agree (assigned value of 2)
   c. Disagree (assigned value of 3)
   d. Strongly Disagree (assigned value of 4)

Part V of V
Last, please fill in a few quick items about yourself. These questions are important for demographic information only.Your answers will be kept completely anonymous.

1. I am ___.
a. Male
b. Female

2. My current age is ___.
a. under 18
b. 18 to 23
c. 24 to 29
d. 30 to 35
e. 36 to 41
f. 42 to 47
g. 48 or older

3. Currently, I am a RIT ___.
a. Undergraduate student
b. Graduate student
c. Alumni
e. Faculty
f. Staff
g. Other

4. I would describe myself as ____.
a. Caucasian
b. African-American
c. Asian-American
d. Native-American
e. Other

5. Are you an international student?
a. Yes
b. No

Are there any concerns about Facebook's privacy policy you would like to add? If so, please use the space below.

Please make sure you have answered all of the questions and then click submit. Thank you for your time and valuable input!