



ISSN: 1946-1836

Journal of Information Systems Applied Research

Volume 3, Number 12

<http://jisar.org/3/12/>

June 7, 2010

In this issue:

A Study of the Perceptions of Students on Privacy and Security on Social Networking Sites (SNS) on the Internet

James P. Lawler

Pace University
New York, NY 10038 USA

John C. Molluzzo

Pace University
New York, NY 10038 USA

Abstract: Social networking on the Internet continues to be a frequent avenue of communication, especially among Net Generation consumers, giving benefits both personal and professional. The benefits may be eventually hindered by issues in information gathering and sharing on social networking sites. This study evaluates the perceptions of information systems and non-information systems students at a leading northeast institution on facets of privacy of marketplace social networking sites, relative to internal information gathering and sharing on the sites. Findings from a survey of the students indicate less knowledge of personal information gathering and sharing techniques on the sites, notably in privacy and security statements, than of the popular sociality of the sites. These findings furnish impetus into the continued improvement of curricula in disciplines of information systems and non-information systems, in order to educate students on often overlooked dimensions of social networking on the Internet.

Keywords: communication technology, curriculum design, cyber-bullying, cyber-stalking, net generation, net geners, privacy, security, social contract theory, social networking, social networking sites, SNS

Recommended Citation: Lawler and Molluzzo (2010). A Study of the Perceptions of Students on Privacy and Security on Social Networking Sites (SNS) on the Internet. *Journal of Information Systems Applied Research*, 3 (12). <http://jisar.org/3/12/>. ISSN: 1946-1836. (A preliminary version appears in *The Proceedings of CONISAR 2009*: §3732. ISSN: 0000-0000.)

This issue is on the Internet at <http://jisar.org/3/12/>

The **Journal of Information Systems Applied Research** (JISAR) is a peer-reviewed academic journal published by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP, Chicago, Illinois). • ISSN: 1946-1836. • First issue: 1 Dec 2008. • Title: Journal of Information Systems Applied Research. Variants: JISAR. • Physical format: online. • Publishing frequency: irregular; as each article is approved, it is published immediately and constitutes a complete separate issue of the current volume. • Single issue price: free. • Subscription address: subscribe@jisar.org. • Subscription price: free. • Electronic access: <http://jisar.org/> • Contact person: Don Colton (editor@jisar.org)

2010 AITP Education Special Interest Group Board of Directors

Don Colton Brigham Young Univ Hawaii EDSIG President 2007-2008	Thomas N. Janicki Univ NC Wilmington EDSIG President 2009-2010	Alan R. Peslak Penn State Vice President 2010	
Scott Hunsinger Appalachian State Membership 2010	Michael A. Smith High Point Univ Secretary 2010	Brenda McAleer U Maine Augusta Treasurer 2010	George S. Nezelek Grand Valley State Director 2009-2010
Patricia Sendall Merrimack College Director 2009-2010	Li-Jen Shannon Sam Houston State Director 2009-2010	Michael Battig St Michael's College Director 2010-2011	Mary Lind North Carolina A&T Director 2010-2011
Albert L. Harris Appalachian St JISE Editor ret.	S. E. Kruck James Madison U JISE Editor	Wendy Ceccucci Quinnipiac University Conferences Chair 2010	Kevin Jetton Texas State FITE Liaison 2010

Journal of Information Systems Applied Research Editors

Don Colton Professor BYU Hawaii Editor	Thomas N. Janicki Associate Professor Univ NC Wilmington Associate Editor	Alan R. Peslak Associate Professor Penn State Univ Associate Editor	Scott Hunsinger Assistant Professor Appalachian State Associate Editor
---	--	--	---

2009-2010 JISAR Editorial and Review Board

Alan Abrahams, Virginia Tech	Mary Lind, NC A&T University	Li-Jen Shannon, Sam Houston St
Ronald Babin, Ryerson Univ	Fortune Mhlanga, Abilene Christian	Michael Smith, High Point Univ
Eric Breimer, Siena College	Monica Parzinger, St Mary's Univ	Karthikeyan Umamathy, U N Florida
Gerald DeHondt II, Grand Valley	Don Petkov, E Conn State Univ	Bruce White, Quinnipiac University
Mark Jones, Lock Haven Univ	Steve Reames, American Univ BIH	Charles Woratschek, Robert Morris
Terri Lenox, Westminster Col	Sam Sambasivam, Azusa Pacific U	Peter Y. Wu, Robert Morris Univ

This paper was in the 2009 cohort from which the top 45% were accepted for journal publication. Acceptance is competitive based on at least three double-blind peer reviews plus additional single-blind reviews by the review board and editors to assess final manuscript quality including the importance of what was said and the clarity of presentation.

© Copyright 2010 EDSIG. In the spirit of academic freedom, permission is granted to make and distribute unlimited copies of this issue in its PDF or printed form, so long as the entire document is presented, and it is not modified in any substantial way.

A Study of the Perceptions of Students on Privacy and Security on Social Networking Sites (SNS) on the Internet

James P. Lawler
lawlerj@aol.com

John C. Molluzzo
jmolluzzo@pace.edu

Pace University
163 William Street
New York, New York 10038 USA

Abstract

Social networking on the Internet continues to be a frequent avenue of communication, especially among Net Generation consumers, giving benefits both personal and professional. The benefits may be eventually hindered by issues in information gathering and sharing on social networking sites. This study evaluates the perceptions of information systems and non-information systems students at a leading northeast institution on facets of privacy of marketplace social networking sites, relative to internal information gathering and sharing on the sites. Findings from a survey of the students indicate less knowledge of personal information gathering and sharing techniques on the sites, notably in privacy and security statements, than of the popular sociality of the sites. These findings furnish impetus into the continued improvement of curricula in disciplines of information systems and non-information systems, in order to educate students on often overlooked dimensions of social networking on the Internet.

Keywords: communication technology, curriculum design, cyber-bullying, cyber-stalking, net generation, net geners, privacy, security, social contract theory, social networking, social networking sites, SNS

1. INTRODUCTION

Social networking on the Internet, the concern of this study, has several definitions. A social network is defined as a location at which consumers create a home page or personal space, on which they blog on Web logs, post files, and share files, ideas and information with other individuals and other networks and sites on the Internet (Turban, King, McKay, Marshall, Lee and Viehland, 2007). Files may be music, photography and video with numerous other utilities (Delehanty, 2009). Salaway (Salaway, Caruso and Nelson, 2008, p. 20) essentially defines a social network site as an extended, functionally improved and larger managed network of other individuals and sites – “all my

people right here, right now” (Lampinen, Tamminen and Oulasvirta, 2009). Snyder (Snyder, Carpenter and Slauson, 2006) defines a social networking site (SNS) as a fundamental social network that may be a frequent and further initiator medium of informal networking relationship (Dickerson, 2004) or a medium of possibility of networking relationship as a social network (Boyd and Ellison, 2007).

The Educase Center for Applied Research (ECAR) Study of Undergraduate Students and Information Technology in 2008 indicates Bebo, Facebook, Friendster, LinkedIn, MySpace, Other, Sconex, Windows Live Space, and Yahoo! 360 as the choices of sites among Net Generation (Echo Boomers, Millennials or Net Geners) consumers aged

32–12 years (Salaway, Caruso and Nelson, 2008, p. 84), as indicated in Figure 1 in Appendix A. Facebook (www.facebook.com) and MySpace (www.myspace.com) are indicated to be the choicest among the consumers at 110 million active users monthly, Facebook is the largest social networking site (Hempel, 2009, p. 37) in the country, almost equivalent to the population of Brazil (Hempel, 2009, p. 35). More than half of teens aged 17–12 years on the Internet are consumers (Digital Communities, 2007), and most students aged 18–19 years are consumers of these sites (Salaway, Caruso and Nelson, 2008, p. 15). More than half of students at academic institutions are on the sites 1 to 5 hours weekly, and a quarter of students are on them 6–10 hours weekly (Salaway, Caruso and Nelson, 2008, p. 15), but 90% are on the sites daily (Sausner, 2009). Students are clearly active consumers of social networking sites, as further indicated in Figure 2 in Appendix A, and the sites are considered to be changing the fabric of institutions (Salaway, Caruso and Nelson, 2008, p. 9) in enabling formation of multiple relationships.

Through social networking sites, students contact family and friends (Lenhart and Madden, 2007), and especially male students in meeting new friends (Salaway, Caruso and Nelson, 2008, p. 15). They learn about other individuals they may not meet in person. They share ideas, information and files with other friends, individuals and especially fellow students (Salaway, Caruso and Nelson, 2008, p. 15). Throughout political seasons, they invite if not mobilize other people and students to programs (McGirt, 2009). They mourn and support themselves in tragedies, such as at Virginia Tech. These sites are definitely facilitating social relationships and resources and are considered a fixture for students.

Social networking sites are enabled through personal profiles (Lehnert and Kopec, 2008) that link to other profiles through protocols on the system. Profiles, exceeding 100 million on MySpace (Solove, 2008, p. 102), consist generally of information on 'about me', ages (including birthdays), ethnicity, habits (drinking and smoking) or interests (holiday or spring break plans), martial conditions (in a relationship), locations (cell numbers, e-mail numbers or instant messaging names), names (pseudonyms), orien-

tations (heterosexual or homosexual), photographs, and religions of the students. Though more than half of students have personal profiles, most students, especially female teenagers, have profiles that are private or semi-private or have other restrictions on the sites (Digital Communities, 2007). Students appear not to be cavalier about disclosing information.

The concern of the authors of this study is that Net Generation students may lack knowledge of the fact, or impact of the fact, that characteristics of social networking sites are inherently public on the World Wide Web. Literature indicates Net Generation students lack knowledge of personal privacy and security on social networking sites (Wilson, 2008), if not knowledge of the privacy and security statements on the sites (Pollach, 2007), as privacy may be perceived to be obsolete in an open society (Brin, 1998). Profiles may be inadvertently divulging intimate information (Solove, 2008, p. 101) on the public sites (Acquisti and Gross, 2005). Students interact and share in instant but intimate information on social networking sites (Tapscott, 2008). These data may be disseminated to audiences on Web or non-Web forums in an unexpected (Kluth, 2009) if not harmful (Brenner, 2009) manner. Such audiences may include advertisers (Claburn, 2007, p. 72), criminals (Kirchheimer, 2009), future employers, governmental investigators, marketing firms (The Economist, 2007), third party organizations that are partners of the sites (Claburn, 2007, p. 69), predators (Consumer Affairs, 2006) or strangers, all of whom might have accounts on the site (Romano, 2006). This further invades privacy on sites that intersect personal and professional information (Snyder, Carpenter and Slauson, 2006). In short, the authors contend that students and teens may not be fully knowledgeable of privacy and security on social networking sites.

2. BACKGROUND

This study attempts to clarify the knowledge of students on issues of privacy and security on public social networking sites. Knowledge of privacy begins with definitions of accessibility privacy, decisional privacy, and informational privacy. Accessibility privacy is defined as freedom from intrusion; decisional privacy is freedom from interference

in personal choices; and informational privacy is freedom to limit access to collection and to control the flow of personal information (Tavani, 2004). Privacy is essentially the right to determine the distribution of private information (Westin, 1967). Inasmuch as protection of privacy is not included as a right in the Constitution of the United States, but is in legal precedents and regulations that have limited protection (Solove, 2008, p. 104) that has to be further safeguarded in society (Lawler, Molluzzo and Vandeputte, 2008), students have to be dependent inevitably on privacy policies of social networking sites.

Social networking sites' privacy policies are effectively social contracts cited in social contract theory (Snyder, Carpenter and Slauson, 2006). Students are dependent on the rules (terms of usage) defined in the policies on the sites. Policies may be designed in favor of the social networking sites, not in favor of the students. Difficulty in interpretability of collection and distribution of information policies in privacy and security statements is clear in practitioner and scholarly literature (Rapoza, 2008 & Showalter, 2008). Importantly the impact of improvement in personal information gathering techniques, information mining technologies, and increased interest in SNS and third-party gathering of private information (Henderson and Snyder, 1999) is not evident in the privacy statements of the sites. Finally, it is not evident in the feasibility of intrusion into the right to privacy and security of the students (Milberg, Smith and Burke, 2000).

Issues of privacy and security statements relative to social networking sites are evident further in the literature. Firms managing the sites are focused less on privacy (McCreary, 2008) and more on marketing opportunities – a \$1.4 billion (Aguiar, 2008) monetization machine at Facebook, MySpace and other social networking sites (Hempel, 2009, p. 37). In the past Facebook has gathered presumed private information without permission of students and informed 'friends of a friend' of students on sites, in order to market products of organizations partnered with Facebook (Gohring, 2008). eGuardian has introduced age clarification methods that may be marketing products to teens with presumed private profiles on MySpace sites without permission of the teenagers (Stone,

2008). Google is introducing monitoring 'friends of a friend' of students that may be influencing the marketing of products on social networking sites (Green, 2008) and is noted for "Web bugs" that share information with others (Rapoza, 2009). Literature indicates students and teenagers may not be fully knowledgeable of marketplace non-privacy on Web sites (Turow, Hennessy and Bleakley, 2008) if not SNS (Havenstein, 2008), even assuming knowledge of privacy and security. Privacy loss may be a loss of security (Dyson, 2008). Moreover, regulations and statements may not be protective of privacy and security (Feretic, 2008), as they may not be current with mining techniques (Markoff, 2008) or technologies (Landau, 2008 & Schneider, 2009).

Such issues are evident in the aforementioned Educase Center for Applied Research (ECAR) Study of Undergraduate Students and Information Technology, in which leaving a history that may cause problems, misusing information of students, security and stalking of students were identified to be problems of social networking sites (Salaway, Caruso and Nelson, 2008, p.16), as indicated in Figure 3 in Appendix A. The extent of the issues in the minds of the students may be a problem, as barely half of the students indicated the issues to be problematical or risky to them (Salaway, Caruso and Nelson, 2008, p. 16). Further surveys indicated that more than half of students are satisfied with privacy and security statements (Harris Poll, 2008). Students may not be fully knowledgeable in information gathering and sharing techniques that may not be furnished in non-interpretable privacy and security statements (McGrath, 2008). They may be generally insensitive to issues of privacy and security (Brown, 2008). This prompts study of student perceptions of the privacy protection in SNS privacy and security statements.

Therefore, the authors attempt to document student knowledge in privacy and security on social networking sites. This study enables a foundation for educators that may enhance curricula for dimensions of exposure on social networking on the Internet (Dhillon and Blackhouse, 2001). This is important as firms in industry invest more in relationships (Baker, 2009) and services (Sausner, 2009) on social networking sites (Greengard, 2008). Students may learn im-

proved methods of personal profiling that might protect privacy and security on the sites (Rennie, 2008). They may learn methods for evaluating elements of fair practices protective of privacy and security (Anton, Bertino, Li and Yu, 2007) evident or not evident in the privacy and security statements of SNS (McGrath, 2008), and for learning which sites furnish the optimum in protection of personal privacy and security. This study furnishes input on the perceptions of privacy and security that can be integrated into curricula that might be more cognizant of the impact of social networking on the Web.

3. FOCUS OF STUDY

The focus of the study is to evaluate the extent of knowledge of Net Generation students in dimensions of information gathering, profiling and sharing in social networking on the Internet. The study explores knowledge of information systems and non-information systems students in SNS privacy practices, particularly as furnished in privacy and security statements on the sites. This study explores the personal practices of the students as they pertain to privacy and security on the sites. Fresh input into the knowledge of privacy and security will help instructors to integrate pedagogical methods reflective of frequently perceived issues of privacy (Clifford, 2009) and of issues of public sharing on social networking sites (Solove, 2008). Learning the problems and risks of invasive technologies (Baase, 2008) will help to protect the privacy of students.

4. RESEARCH METHODOLOGY

The survey was conducted during May and June 2009. It was administered online to graduate computing students and undergraduate students in several disciplines at Pace University, New York City. Of approximately 1200 students asked to participate in the study (most by email, some in several classes), 110 valid responses were obtained.

Survey Instrument

The survey consisted of several demographic data questions. These were followed by questions to discover what kind of data students post on their social networking sites (SNS), and questions that asked about student knowledge how their social networking

sites handle their personal information. Many questions from the survey will be discussed in the following section. There were five demographic questions, one question asking which SNS the respondent belongs to, and one question that asked how many hours the respondent spends each week on their SNS. Question 8, henceforth referred to as the "Data Question", listed fifteen types of data a respondent might place on their SNS. Questions 9 through 20, henceforth referred to as the "Knowledge Questions", asked about the respondent's knowledge about their SNS privacy policy, and if they had read that policy. The complete survey instrument is available from the authors. For reference in the following, the Data and Knowledge Questions are included in Appendix B.

Demographic Data

During May and June, 2009 110 students were surveyed. Graduate (45%) and undergraduate (55%) students were included in the study. Most of the respondents (68%) were computing students. The average age of the respondents was 27.8. The ethnicity was distributed as follows: African American (9%), Asian (26%), Caucasian (33%), Hispanic (20%), Middle Eastern (3%), and other (9%). Most of the respondents were male (62%).

Respondents were asked to choose among a list of 10 popular social networking sites. The three most popular were Facebook (82% were members), MySpace (35% were members), and LinkedIn (30% were members.) Respondents were asked how many hours they spend each week on their SNS. Our data confirm the results of Salaway (Salaway, Caruso and Nelson, 2008, p. 15) in that more than half of students (67% in the current survey) spend 1 to 5 hours each week on SNS, and about one-quarter (23% in the current survey) spend between 5 and 10 hours each week on SNS.

Data Stored on Social Networking Sites

Respondents were asked to select from a list the types of data they store on their social networking sites. The results are shown in Table 1 in Appendix C, which shows the percent of the respondents who indicate they store that type of data.

Note that nearly everyone stores their name (93%) and gender (93%). Many store the names of friends (81%), photos (78%), and age (71%). A surprising number store what can be considered highly personal data, such as their telephone number (17%) and address (16%).

The survey asked whether the respondent's profile was public (i.e. available to anyone who is a member of the SNS and in some instances, for example MySpace, to anyone on the Internet), or private (available only to those SNS members "friended" or invited by the respondent.) Among the respondents, 54% indicated that their profile was private; 38% indicated that it was public; and 8% did not know!

5. ANALYSIS AND DISCUSSION

Background

The survey contained questions that asked about the respondent's knowledge of how their personal information is gathered, used, and shared. The survey also asked questions about choices SNS users have about the accuracy and security of personal information gathered by their SNS. See Appendix B for a list of the questions used in the survey. In these questions, respondents were asked to respond "yes", "don't know", or "no." Because our sample size was relatively small ($n = 110$), having three categories did not yield statistically valid results. It was felt that the "don't know" and the "no" responses basically meant the same thing – the respondent could not answer in the affirmative. Therefore, these answers were combined, which enabled a chi-squared test of significance on 2x2 cross-tabs. Following is an analysis of some of the statistically significant results organized along some of the categories of the respondents.

Academic Differences

There were only two significant differences between graduate and undergraduate students. Undergraduate students are more likely to store their name on their SNS than graduate students ($p=.025$), a result that will surely be different in a few years.

Students were asked "Do you have a convenient and easy way to contact the site to correct information gathered about you?" Almost half the undergraduates believe they

do have a way, but less than a quarter of the graduate students believed they do, which is a significant difference ($p=.003$).

There was only one significant difference between computing and non-computing majors. When asked if they include their place of employment on their SNS, about half the computing students answered "yes" as opposed to only one quarter on the non-computing majors. This is a significant difference, with $p=.013$.

Age Differences

Table 2 in Appendix C shows the significant differences between the age groups Age ≤ 23 and Age > 23 . The Question numbers in the table refer to the list of survey questions in Appendix B. Question 8 is a list of things a person might store on a SNS site. There are significant differences in storing school attending, tastes and preferences, relationship status, sexual preferences, and photos. There are significant differences between age groups on questions 15 and 16, which refer to ways of correcting errors on the SNS.

Gender Differences

It is interesting that no significant differences between the sexes were found on any questions. This is a point to which the authors will return in an expanded study of undergraduate students, which will be conducted in the fall 2009 and spring 2010.

Use Differences

Hours of use: Respondents were asked how many hours they spend each week on their SNS. For purposes of comparison, we divided the respondents into two groups: users who spend less than 6 hours per week and users who spend 6 or more hours each week (Salaway, Caruso and Nelson, 2008, p. 15.) The results are shown in Table 3 in Appendix C.

Most of the differences are in Question 8, which concerns the data users place on their SNS. There are significant differences in placing social activities on SNS (Question 8i) where it seems that heavy users (more than 6 hours on SNS) are more likely to place their social activities on their SNS. There are also differences in tastes and preferences, sexual preferences, political views, and religion. Question 12 asked the respondents if

their SNS tells them if their data will be shared with external organizations. As shown in Table 3 of Appendix C, we see that there is a significant difference between the groups at the .05 level of significance, with heavy users more likely to believe their SNS will tell them their data is shared.

Facebook Users: Because 82% of the respondents were Facebook users, the authors decided to see if there were significant differences between these users and non-Facebook users. Table 4 in Appendix C summarizes the significant differences.

As shown in Table 4 of Appendix C, there are significant differences between Facebook and non-Facebook users along several of the data types listed in Question 8. A significant difference at the .001 level occurred in posting relationship status. Significant differences at the .05 level occurred in posting school attending and sexual preferences. In these cases, it appears that Facebook users are more likely to post the data. This is to be expected because of the highly casual social nature of Facebook. It should be noted that there could also be a difference between Facebook and non-Facebook users in posting one's address, gender, friends, photos and political views. These results were not statistically acceptable because of the small sample size of the non-Facebook users. In the study the authors will undertake in the fall 2009 and spring 2010, this will be further investigated.

Privacy Policy Readers: The authors categorized respondents as those who have read their SNS privacy policy and those who have not. Table 5 of Appendix C shows the significant differences between these groups.

Here again are differences in two parts of the data question. Among those who claim to have read their SNS privacy policy, about half place social activities and tastes and preferences on their SNS, as opposed to less than one-third of those who have not read their SNS privacy policy.

More important, however, are the differences in responses to the knowledge questions. There are highly significant differences between the groups in answering questions 11 (SNS sharing data with internal departments) and 14 (Choice about how personal data will be used.) There are differences between the two groups at the .05 level of sig-

nificance in answering questions 10 (SNS tells you how personal data will be used) and 12 (SNS sharing data with external organizations.) Finally, there are differences at the 0.05 level of significance in questions 15 (Having an easy way to contact the SNS to correct personal data) and 18 (what will the SNS do if there is a data breach.) In all these cases, the respondents who read their SNS privacy policy are more likely to claim knowledge about their SNS policies.

6. IMPLICATIONS OF STUDY

Referring to Table 1 in Appendix C, note that the most popular items students place on their SNS concern their personal data and preferences. Data such as name, gender, school attending, friends, and photos are routinely stored by them. However, it is noteworthy that there seems to be some concern among respondents about privacy. For example, only 16% store their address and 17% their telephone number. Also, it seems that respondents are somewhat reluctant to store data that one might consider too personal to make public. For example, only 25% store their political views and 25% store their religion. The implication is that SNS users appear to have three levels of privacy concern. Privacy Level 1, or high privacy, consists of items such as address, telephone number and political views that users tend not to divulge on their SNS. Privacy Level 2, or medium privacy, consists of items to which users seem to be indifferent, such as place of employment, relationship status and social activities. Finally, Privacy Level 3, or low privacy, consists of those items that users freely share with other users of their SNS, such as name, friends, and photos.

The majority of respondents (55.6%) did not read the privacy policies of their SNS. This could be the result of several factors. A user might not care about privacy and, therefore, not seek out the privacy policy. A user might assume their data will be kept private and, therefore, not seek out the privacy policy. The link to the SNS privacy policy might not be easy to find. Even if the user seeks out the policy, it could be too long or written in terms that are difficult to understand thereby encouraging the user not to bother reading it. Whatever the reason, it is clear that SNS should make their privacy policies easily

accessible and easy to read. SNS might also consider trying to make new users read their privacy policy as part of the sign-up process.

The results obtained on the Knowledge Questions show a range of knowledge of SNS privacy policies. Table 6 shows how people responded to the Knowledge Questions. Note the very large percentage of respondents (except for question 19) who did not know the answers! This means that these people either did not read their SNS privacy policy, read it and did not remember, or read it and did not understand it. Again, this confirms the authors' belief that more has to be done by SNS to make their privacy policy statements more accessible to their members. Further study needs to be done to see if there is a correlation between not reading the SNS privacy policy and not knowing the answers to the questions.

Note also that questions 10, 14, 15, 17, and 18 have less than one-third "Yes" responses. Question 10 (does the SNS tell how personal data will be used) elicited only a 33% "Yes" response. Thus 67% of respondent do not know how their personal data might be used by their SNS. Question 14 (do you have a choice in how your data is used) received only a 21% "Yes" response rate, while Question 15 (Do you have an easy way to correct your SNS data) received only a 35% response rate, and Question 18 (what will the SNS do in case of a data breach) received a "Yes" response rate of only 14%. These results imply that users do not know their rights as users of their SNS, thus basically relinquishing control of their personal data.

Also implied in this study is the need for better online privacy education. Nearly all teenagers and college-age people in the U.S. are members of at least one SNS. See Figure 2 in Appendix A. The present study shows that a large part of this population is unaware of the data practices of their SNS. This population needs to be educated on how their SNS, indeed nearly all Internet sites, collect and use their surfing and personal data. Most colleges and universities have introductory computing courses. These courses should include modules on privacy and the Web. Our nation's high schools should also educate their students, who all too frequently are very open about what they store on their SNS, on who might see their personal data, how permanent that

data is on the Internet, and how their SNS might use their personal data.

7. LIMITATIONS AND OPPORTUNITIES

The present study has several limitations. First, the sample size (110) is small and, relative to the sample size, has too many graduate students (45%). In the fall 2009 and spring 2010, the authors will conduct a larger study. It is hoped that an additional 200 to 300 undergraduates will be surveyed. Because current undergraduate students have "grown up" using social networking, more significant data should be collected. Results of this study will reported in a future paper.

The answers to the knowledge questions in the survey (for example question 9 asks, "Do you know what personal information your Social Network site gathers?"), must be interpreted with caution. If a respondent answered that they read their SNS privacy policy (question 20, 44% claimed they did), then what does it mean if they answered "Yes" to question 9? Does their SNS privacy statement actually state what personal information it will gather, or does the student merely think that the SNS privacy policy makes this statement? In the fall 2009 and spring 2010, the authors will study whether what survey respondents think is stated in their SNS privacy policy is in fact actually stated in that policy.

Another opportunity for further research is to verify the three levels of privacy mentioned in Section 6. A study involving many more respondents could verify or refine this. Moreover, research needs to be done to verify the conclusion that not knowing the answers to the Knowledge Questions is related to not reading the SNS policy statements.

8. CONCLUSION

Results of this study show that many respondents have not read their SNS privacy policy statement. It also shows that many do not know how their personal information will be gathered, used, and shared. Finally it also shows respondents are not familiar with their rights regarding their own personal data stored on SNS. Clearly, SNS need to make privacy more of a priority than it is now. Users need to be informed in easily

accessible privacy statements that are easy to understand – especially by teenagers who make up a substantial proportion of their users.

SNS frequently point out that a user can customize their privacy settings very easily. However, what is easy to one may not be to another. For example, to control what certain groups of people can see on a page, Facebook allows a user to create lists of friends. Using lists, a user can restrict sharing of content to certain lists. This sounds like an effective way to control who sees what content on a user's page. Actually creating the restricted lists, however, is not so easy. Described as a "little known feature", here is how it is done.

"To create a list, click on the *Friends* link, and under "Lists" on the left, click *Create*. To restrict sharing info in certain lists, go to *Settings/Privacy Settings* and click *Profile*. Open a profile item's drop-down menu and choose *Customize*. Select *Some Friends* in the resulting pop-up, and then enter the name of the friends list you want to choose. (Larkin, 2009)

Thus, Facebook does not make it as easy as it could to create and manage restricted lists of friends. Why does this have to be so difficult to do?

SNS, and most other Websites, are in business to make money. One way to do so is to use the data gathered, personal data in the case of SNS, for profit. The amount of personal data contained on a SNS is enormous. This data has great value to marketers. Facebook's Beacon is an example of how such data can be used. First offered as an opt-out service, Beacon shared Facebook users' purchases from affiliated companies with their Facebook friends. So, for example, if you bought a book from an affiliate online bookstore, that purchase would be known to one's Facebook friends. The existence of this service caused an uproar among Facebook users, spurred on by an online petition against Beacon by the civil action group MoveOn.org. As a result, Facebook made the service opt-in (Blodget, 2007). While this story has a more or less "happy ending", it does emphasize that user data on SNS is basically for sale. This fact needs to be made know to SNS users.

Perhaps the best way to ensure that the public is made aware of SNS privacy concerns is through proper education. This education needs to take place at all levels. Although many SNS require that their members be at least 13 years of age to join, many pre-teens use SNS, such as MySpace, to keep in touch with friends. Thus educating pre-teens and their parents on the importance of what data is stored on their SNS, how it might be used, and who is likely to have access to it is very important. Once in high school where there is usually a great increase in social activity, students should again be educated about their personal data stored on SNS. Finally, as students prepare for their entrance into the workforce, they should be educated on the consequences of posting inappropriate personal data on their SNS.

9. REFERENCES

- Acquisti, A. and Gross, R. (2005) "Information Revelation and Privacy in On-Line Social Networks" Electronic Society Conference, Alexandria, Virginia, November 7.
- Aguiar, Y. (2008) "The On-Demand Generation: Adapting to Today's Globalized Customer and User Needs" Tri-State CIO Forum, Intel / eMarketer, Presentation, May 7.
- Anton, A.I., Bertino, E., Li, N. and Yu, T. (2007) "A Roadmap for Comprehensive On-Line Privacy Policy Management" Communications of the ACM, 50(7), pp. 109-115.
- Baase, S. (2008) A Gift of Fire: Social, Legal and Ethical Issues for Computing and the Internet, 3rd Edition. Pearson Prentice Hall, Upper Saddle River, New Jersey, p. 45.
- Baker, S. (2009) "What's a Friend Worth?: Companies Are Scrambling to Decode New Data about Our On-Line Relationships, Hoping for Profitable Insights" Business Week, June 1, pp. 032-036.
- Blodget, H. (2007) "Facebook's 'Beacon' Infuriate Users, MoveOn" Silicon Valley Insider, 21, November
www.alleyinsider.com/2007/11/facebooks-beaco.html, last accessed June 19, 2009.
- Boyd, D.M. and Ellison, N.B. (2007) "Social Network Sites: Definition, History, and

- Scholarship" *Journal of Computer-Mediated Communication*, 13(1), pp. 210-230.
- Brenner, B. (2009) "Slapped in the Facebook: Social Networking Dangers Exposed" *CSO*, March, p. 9.
- Brin, D. (1998) *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom*. Perseus Books, New York.
- Brown, P. (2008) "Privacy in an Age of Terabytes and Terror" *Scientific American*, September, p. 46.
- Claburn, T. (2007) "Call off the Wolves: It Is Time to Give Customers Control over All That Data You Are Collecting on Them" *Information Week*, November 12, p. 69.
- Claburn, T. (2007) "Social Networks Have Data to Share" *Information Week*, November 12, p. 72.
- Clifford, S. (2009) "Many See Privacy on Web as Big Issue, Survey Says" *The New York Times*, March 16, pp. 1-2.
- Delehanty, H. (2009) "Confessions of a Facebook Addict", *AARP*, July & August, pp. 41-43.
- Dhillon, G. and Blackhouse, J. (2001) "Current Directions in Information Systems (IS) Security Research" *Information Systems Journal*, 11(2), pp. 127-153.
- Dickerson, C. (2004) "Make the Right Connections: Social Networking Offers a Productive Way to Expand Professional Contacts" *Infoworld*, January 26, p. 22.
- Dyson, E. (2008) "Reflections on Privacy 2.0" *Scientific American*, September, p. 50.
- Feretic, E. (2008) "Nowhere to Hide: Managers Should Play a Major Role in Ensuring That Their Companies Adhere to Ethical Privacy Policies" *Baseline*, September, p. 10.
- Gohring, N. (2008) "Facebook Faces Class-Action Suit" *CIO*, August 13, pp. 1-6.
- Green, H. (2008) "Google: Harnessing the Power of Cliques" *Business Week*, October 6, p. 050.
- Greengard, S. (2008) "Flying High with Social Networking", *Baseline*, October 30, pp. 1-2.
- Havenstein, H. (2008) "Millennials Demand Changes in Information Technology (IT) Strategy" *Computerworld*, p. 13.
- Hempel, J. (2009) "How Facebook Is Taking Over Our Lives" *Fortune*, March 2, p. 35,37.
- Henderson, S. and Snyder, C. (1999) "Personal Information Privacy: Implications for Management Information Systems (MIS) Managers" *Information and Management*, 36, pp. 213-220.
- Kluth, A. (2009) "The Perils of Sharing: The Surprising Threat to Your Privacy Is Closer Than You Think" *The World in 2009*, *The Economist*, January, p. 28.
- Kirchheimer, S. (2009) "False Friends: ID Thieves 'Are Clearing Investing Time and Resources on Social Networks'" *AARP Bulletin*, June, p. 16.
- Lampinen, A., Tamminen, S. and Oulasvirta, A. (2009) "All My People Right Here, Right Now': Management of Group Co-Presence on a Social Networking Site" *Communications of the ACM Proceedings of Group '09 Conference*, Sanibel Island, Florida, May 10-13.
- Landau, S. (2008) "Privacy and Security: A Multidimensional Problem" *Communications of the ACM*, 51(11), pp. 25-26.
- Larkin, E. (2009) "Privacy Watch" *PC World*, July 9, p. 38.
- Lawler, J., Molluzzo, J. and Vandeputte, P. (2008) "An Expanded Study of Integrating Issues of Location-Based Privacy with Mobile Computing into General Curriculum of Universities" *Information Systems Education Journal (ISEDJ)*, 6(47), p. 5.
- Lehnert, W.G. and Kopec, R.L. (2008) *Web 101*, 3rd Edition. Pearson Addison Wesley, Boston, Massachusetts, p. 248.
- Lenhart, A. and Madden, M. (2007) "Teens, Privacy and On-Line Social Networks" *Pew Internet and American Life Project Report*, 2007, April 18.
- Markoff, J. (2008) "You Are Leaving a Digital Trail. Should You Care?" *The New York Times*, Sunday Business, November 30, pp. 1,7.
- McCreary, L. (2008) "What Was Privacy?: Privacy as We Knew It Is Virtually Gone.

- Why Should You Care? What Should Your Business Do about It?" Harvard Business Review, October, p. 124.
- McGirt, E. (2009) "Boy Wonder: The Untold Story of How Chris Hughes Helped Create Two of the Most Successful Startups in Modern History, Facebook and the Obama Campaign" Fast Company, April, pp. 59-97.
- McGrath, L.C. (2008) "Social Networking and Privacy: The Dichotomy" Proceedings of the Southeastern Information for Operations Research and the Management Sciences (INFORMS) Conference, October, Myrtle Beach, South Carolina, p. 477.
- Milberg, S., Smith, H. and Burke, S. (2000) "Information Privacy: Corporate Management and National Regulation" Organization Science, 11(1), pp. 35-57.
- Pollach, I. (2007) "What's Wrong with On-Line Privacy Policies?" Communications of the ACM, 50(9), pp. 103-108.
- Rapoza, J. (2009) "Web Bug Alert: Web Bugs Spread by the Likes of Google Can Make Your Privacy Sick" eWeek, June 15, p. 21.
- Rapoza, J. (2008) "'Privacy Policy' as Oxymoron: Current United States (US) Law Prevents Real Progress in the On-Line Privacy Push" eWeek, October 20, p. 48.
- Rennie, J. (2008) "Seven Paths to Privacy: History Is Ambiguous about Government Willingness to Protect Private Life, but a Few Recommendations Can Help Keep Its Future Secure" Scientific American, September, p. 37.
- Romano, A. (2006) "Walking a New Beat: Surfing MySpace.Com Helps Cops Crack the Case" Newsweek, April 24, p. 48.
- Salaway, G., Caruso, J.B. and Nelson, M.R. (2008) "The Educause Center for Applied Research (ECAR) Study of Undergraduate Students and Information Technology, 2008" Educause Center for Applied Research, 8, pp. 9,15,16,20,26,83,84,93.
- Sausner, R. (2009) "Generation Y's Tastes in Internet Delivery" Bank Technology News, March, p. 15.
- Sausner, R. (2009) "Some Say Twitter's for the Birds" Bank Technology News, May, p. 22.
- Schneider, G.P. (2009) Electronic Commerce, 8th Edition, Course Technology Cengage Learning, Boston, Massachusetts, pp. 343,345.
- Showalter, E.D. (2008) "Privacy Policies: An Investigation into Best Practices for Information Security and Data Protection" Proceedings of the Southeastern Information for Operations Research and the Management Sciences (INFORMS) Conference, October, Myrtle Beach, South Carolina, p. 851.
- Snyder, J., Carpenter, D. and Slauson, G.J. (2006) "MySpace.Com – A Social Networking Site and Social Contract Theory" Proceedings of the Information Systems Education Conference (ISECON), 23 (3333), Dallas, Texas, pp. 2-3.
- Solove, D.J. (2008) "The End of Privacy: Young People Share the Most Intimate Details of Personal Life on Social Networking Web Sites, Portending a Realignment of the Public and the Private" Scientific American, September, pp. 101-102,104.
- Stone, B. (2008) "No Adults Allowed. (Marketers Welcome.)" The New York Times, Sunday Business, November 16, p. 1.
- Tapscott, D. (2008) Grown Up Digital: How the Net Generation Is Changing Your World. Mc-Graw-Hill, New York.
- Tavani, H.T. (2004) Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology. John Wiley and Sons, Hoboken, New Jersey, pp. 92,121,124,140,144,146.
- Turban, E., King, D., McKay, J., Marshall, P., Lee, J.K. and Viehland, D. (2007) Electronic Commerce: A Managerial Perspective, 2008. Prentice Hall, Upper Saddle River, New Jersey.
- Turow, J., Hennessy, M. and Bleakley, A. (2008) "Consumers' Understanding of Privacy Rules in the Marketplace" Red Orbit, October 2, pp. 4-6.
- Westin, A. (1967) Privacy and Freedom. Atheneum Publishers, New York.
- Wilson, T. (2008) "Your Biggest Threat: Gen Y" Information Week, December 1, p. 20.
- _____ (2008) "Comfort of United States (US) Internet Users" Harris Poll, Harris Interactive, April.

_____ (2007) "Word of Mouse: Will Facebook, MySpace and Other Social Networking Sites Transform Advertising? The Economist, November 10, p. 77-78.

_____ (2007) "Study: Majority of On-Line Teens Use Social Networks and Have Created On-Line Profiles" Digital Communi-

ties: Building 21st Century Communities, Pew Internet Project Survey, January 12, pp. 1-5.

_____ (2006) "Connecticut Opens MySpace.Com Probe" Consumer Affairs, February 5.

APPENDICES

APPENDIX A: FIGURES ON SOCIAL NETWORKING SITES

Social Networking Sites	Age of Consumers		
	18-19 Years (n=8,705)	20-24 Years (n=10,929)	25-29 Years (n=1,381)
Facebook	95.5%	92.9%	60.6%
MySpace	44.0%	45.1%	79.5%
Other	8.2%	7.8%	13.7%
Yahoo! 360	2.3%	1.9%	6.6%
Windows Live Space	3.0%	2.0%	3.5%
LinkedIn	0.4%	3.1%	5.0%
Friendster	0.9%	1.5%	4.3%
Bebo	1.2%	0.9%	0.7%
Sconex	0.2%	0.1%	0.1%

FIGURE 1: SOCIAL NETWORKING SITES – CHOICES OF CONSUMERS (STUDENTS)

Source: Salaway, G., Caruso, J.B. and Nelson, M.R. (2008), The Educause Center for Applied Research (ECAR) Study of Undergraduate Students and Information Technology, 2008. Research Study from Educause Center for Applied Research, 8, p. 84 [Adapted].

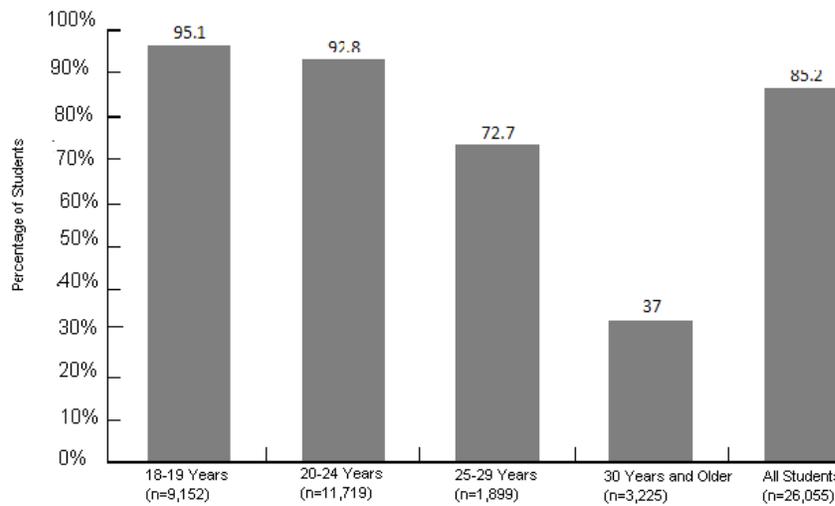


FIGURE 2: SOCIAL NETWORKING SITES – GENERATION OF CONSUMERS (STUDENTS)

Source: Salaway, G., Caruso, J.B. and Nelson, M.R. (2008), The ECAR Study of Undergraduate Students and Information Technology, 2008. Research Study from Educause Center for Applied Research, 8, p. 83.

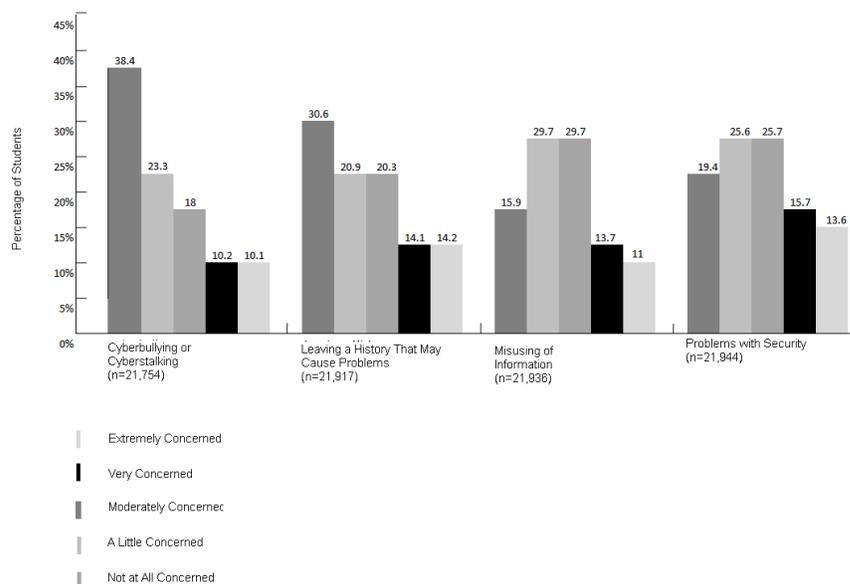


FIGURE 3: SOCIAL NETWORKING SITES – ISSUES ON PRIVACY AND SECURITY

Source: Salaway, G., Caruso, J.B. and Nelson, M.R. (2008), The ECAR Study of Undergraduate Students and Information Technology, 2008. Research Study from Educause Center for Applied Research, 8, p. 93 [Adapted].

APPENDIX B: INSTRUMENT OF SURVEY

Following are the non-demographic survey questions only.

8. What information do you have on your Social Networking site? Check all that apply.
 - a. Name
 - b. Address
 - c. Telephone Number
 - d. Age
 - e. Gender
 - f. School Attending
 - g. Place of Employment
 - h. Friends
 - i. Social Activities
 - j. Tastes and preferences
 - k. Relationship Status
 - l. Sexual Preferences
 - m. Photos
 - n. Political Views
 - o. Religion
9. Do you know what personal information your Social Network site gathers?
10. Does your Social network site tell you explicitly how the site will use your data?
11. Does your Social Network site tell you if your information will be shared with other internal departments and personnel of the business of this site?
12. Does your Social Network site tell you if your information will be shared with other external firms or organizations partnered with the business of this site?
13. Do you have a choice about the amount of information your Social Networking site gathers about you?
14. Do you have a choice about how the information gathered about you will be used?
15. Do you have a convenient and easy method to contact the site to correct information gathered about you?
16. Do you have the ability to review and correct information gathered about you?
17. Do you know how your information will be safeguarded?
18. Do you know what the site will do if there is a breach in the security of the site?
19. Is your profile public? That is, can any other site user access your profile, friend or not?
20. Have you read the privacy policy of your Social Networking site?

APPENDIX C: STATISTICAL TABLES**TABLE 1 - DATA STORED ON SNS**

Data Stored	Percent Choosing
Name	93%
Address	16%
Telephone Number	17%
Age	71%
Gender	93%
School Attending	72%
Place of Employment	42%
Friends	81%
Social Activities	44%
Tastes and Preferences	33%
Relationship Status	59%
Sexual Preferences	41%
Photos	78%
Political Views	25%
Religion	25%

**TABLE 2 – SIGNIFICANT DIFFERENCES BETWEEN
AGE ≤ 23 AND AGE > 23**

Question	p ≤ .001	p < .01	p < .05
8f		.005	
8j			.039
8k	.001		
8l			.039
8m			.019
15			.012
16		.008	

**TABLE 3 – SIGNIFICANT DIFFERENCES BETWEEN
HOURS < 6 AND HOURS ≤ 6 SPENT ON SNS**

Question	$p \leq .001$	$p < .01$	$p < .05$
8i		.005	
8j			.012
8l			.017
8n			.011
8o			.038
12			.032

**TABLE 4 – SIGNIFICANT DIFFERENCES BETWEEN
FACEBOOK AND NON-FACEBOOK USERS**

Question	$p \leq .001$	$p < .01$	$p < .05$
8f		.002	
8k	.000		
8l		.003	

**TABLE 5 – SIGNIFICANT DIFFERENCES BETWEEN
READERS AND NON-READERS OF SNS PRIVACY POLICY**

Question	$p \leq .001$	$p < .01$	$p < .05$
8i			.027
8j	.001		
10		.004	
11	.001		
12		.002	
14	.000		
15			.038
18			.029

TABLE 6 – PERCENT RESPONSES TO THE KNOWLEDGE QUESTIONS

Question	Yes	Don't Know	No
9	51	36	13
10	33	46	21
11	37	49	14
12	37	50	13
13	47	42	10
14	21	55	23
15	35	46	19
16	40	43	18
17	26	42	32
18	14	42	44
19	38	8	54