An Expanded Study of Net Generation Perceptions on Privacy and Security on Social Networking Sites (SNS)

James P. Lawler
lawlerj@aol.com

John C. Molluzzo
jmolluzzo@pace.edu

Vijal Doshi
vd72618n@pace.edu

Pace University
Seidenberg School of Computer Science and Information Systems
1 Pace Plaza
New York, New York 10038

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 students taking a required university-core computing course in an expanded and new survey 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 the survey continue to demonstratively 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 the 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, photographs 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 Educause 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 12-32 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 the top choices among the consumers at 110 million active users monthly; Facebook is the largest social networking site (Hempel, 2009, p. 37) in the country, with user base almost equivalent to the population of Brazil (Hempel, 2009, p. 35). Facebook is now the second most popular site on the Internet after Google (The Economist, 2010). More than half of teens aged 12–17 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), marital statuses (in a relationship), locations (cell numbers, e-mail addresses or instant messaging names), names (pseudonyms), orientations (heterosexual or homosexual), photographs, and religions of the students. Though more than half of the 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**.** In addition, because of the nomenclature (e.g. "MySpace"), students may be induced into a false impression of privacy and security (Mooradian, 2009). 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), more than older generations (Zukowski and Brown, 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 instant but intimate information on social networking sites (Tapscott, 2008), including information disseminated by friends (Ho, Maiga and Aimeur, 2009) and by friends of adversaries (Nagle and Singh, 2009). 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), strangers, or stalkers (Paullet, Rota, Turchek and Swan, 2009) or almost any audiences (Rosenblum, 2007), 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). Privacy risk is significant (Whitcomb and Fiedler, 2010). In short, the authors contend that students and teens may not be fully knowledgeable of privacy risk 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 the collection and control the flow of personal information (Tavani, 2004). On-line privacy "is the continuous process of negotiating with relevant third parties, an optimum or acceptable level of disclosure of personal information" on the Web (Moloney and Bannister, 2009). Privacy is essentially the right to determine the distribution of private information (Westin, 1967) "grounded on the more general principle of respect for persons" (Benn, 1971). 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 Vandepeutte, 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, though such rules may be artifacts of the 1990s (Lohr, 2010). 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 engaged in fruitful interactions (Vijayan, 2009), but are focused less on privacy (McCreary, 2008) and more on marketing opportunities (MacMillian, 2009) – 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). Facebook is piloting "digital calling cards" that identify subjects as they surf the Web (MacMillian, 2010). 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 Educause 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 the 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 the 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 in an expanded survey that began in 2009 (Lawler and Molluzzo, 2009). This new survey 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). They invest more and more in snooping of students when they recruit them (Lamm and Phile, 2009). They may not have invested in sufficient privacy training of their staff (Cline, 2010). Students may learn improved 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. The results of the new survey in the present study furnish 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 this study is to further evaluate the extent of knowledge of Net Generation students in dimensions of information gathering, profiling and sharing in social networking on the Internet. As in the preliminary published study of 2009 (Lawler and Molluzzo, 2009), this study explores knowledge of SNS privacy practices among students taking a required core introductory computing course, 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. Updated input into the knowledge of privacy and security will help instructors to integrate pedagogical methods reflective of frequently perceived issues of privacy (Clifford, 2009), issues of public sharing (Solove, 2008), and mechanisms needed on privacy and security on the sites (Strater and Lipford, 2008). Learning the problems and risks of invasive technologies (Baase, 2008) will help to protect the privacy of students. The study in this new survey is timely as pundits not infrequently perceive the problems and risks of social networking technology (Prince, 2010).

4. RESEARCH METHODOLOGY

The survey was conducted during spring and fall 2009, and the findings were evaluated in the spring and summer 2010. It was administered online to undergraduate students who were taking the introductory university-core required computing course. Of approximately 500 students asked to participate in the study (most by email, some in several classes), 384 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 of 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 the fall and spring semesters of 2009 384 students were surveyed. The average age of the respondents was 19.9. The ethnicity was distributed as follows: African American (8.6%), Asian (14.6%), Caucasian (53.1%), Hispanic (13.7%), Middle Eastern (2.2%), and other (7.7%). Most of the respondents were female (60.9%).

Respondents were asked to choose which among a list of 10 popular social networking sites they were members. The three sites that achieved at least 10% were Facebook (95.1% were members), MySpace (30.7% were members), and Twitter (22.4% were members.) Respondents were asked how many hours they spend each week on their SNS. Our data tend to confirm the results of Salaway (Salaway, Caruso and Nelson, 2008, p. 15) in that about half of students (47.9% in the current survey) spend 1 to 5 hours each week on SNS, and about one-quarter (32.8% in the current survey) spend between 5 and 10 hours each week on SNS. Of those surveyed, 8.9% reported that they spend more than 16 hours on their 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 (96.2%) and gender (92.2%). Many store the names of friends (88.4%), photos (86.0%), and age (75.2%). A surprising number store what can be considered highly personal data, such as their telephone number (14.3%), but not many store their address (4.9%).

It is of some interest to consider some of the intersections of these attributes. For example, 50.7% of respondents include in their profile all of the following: name, age, gender, school attending, names of friends, relationship status, and photos. Adding sexual preferences changes the percentage to 30.7%, and then adding religion changes the percent to 16.9%. This would give enough information to a hacker to construct an accurate profile on 1 of every 6 SNS users!

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, 15.6% indicated that it was public. This indicates that the well-publicized concerns over one's privacy SNS profile are having a positive effect on first-year university students.

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 = 384), 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

Pace University consists of five undergraduate schools, including a school of computing. Because computing students *should* be more attune to the privacy dangers inherent in surfing the Web as well as the privacy dangers of SNS, the respondents were separated into computing and non-computing majors to see if there were

indeed any differences between the groups in how they perceive privacy issues on SNS.

Interestingly, there were no significant differences between the groups on any of the Knowledge Questions. Thus, even non-computer majors seem to know as much about their SNS privacy policy as their computing major counterparts.

The only significant differences between these groups were in how much time the students spent online, with the computing students spending more time online ($p = 0.016$), placing on their SNS which school they attend ($P = 0.024$) and their identifying their friends ($p = 0.055$).

Age Differences

The respondents were separated into first-year and non-first-year students. Table 2 in Appendix C shows the significant differences between these groups. 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 age, school attending and place of employment. There are significant differences between age groups on questions 10, 14 and 16. Question 10 asks if their SNS tells them how their data will be used, and question 14 asks if they have a choice in the amount of data gathered about them. Question 16 refers to ways of correcting errors on a SNS.

Gender Differences

There were several significant differences in male and female responses. Table 3 in Appendix C summarizes the results. In the Data Question (question 8), which asks what the respondent has stored on their SNS, males were more likely to store their telephone number (8c) and to list their sexual preferences (8l), while females were more likely to list friends (8h) and their relationship status (8k).

On question 10, which asks if the respondent knows how their SNS uses their personal data, and question 16, which asks if the respondent knows how to correct information gathered by their SNS, males are more likely to answer yes. On question 11, which asks if the respondent knows if their information will be shared internally, and question 12, which asks if the respondent knows how their information is shared external to the SNS, females are more likely to answer yes.

Ethnicity Differences

Pace University is ethnically very diverse. Among those surveyed, 51% were Caucasian, 15% Hispanic, 13 % Asian, 8% African American, and the remaining 13% divided among other ethnicities. For purposes of analysis, the respondents were divided between Caucasian and Minorities. The significant differences between these groups are summarized in Table 4 in Appendix C.

There were two significant differences at the $p = 0.05$ level in the Data Question. Minorities stored their addresses (8b) significantly more than Caucasians, but Caucasians listed their sexual preferences (8l) significantly more than Minorities. This is perhaps a reflection of more liberal sexual attitudes in the West.

There were also significant differences at the $p = 0.05$ level in three of the Knowledge Questions. Minorities were more likely to respond that they knew what data their SNS gathered (question 9), and that they believed their SNS explicitly tells them how their data is used (question 10). However, Caucasians are more likely to respond that their SNS tells them if their information will be shared internally (question 11).

Hours of Use Differences

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 (light users) and users who spend 6 or more hours each week (heavy users) (Salaway, Caruso and Nelson, 2008, p. 15.) The results are shown in Table 5 in Appendix C.

Most of the differences are in the Data Question – question 8. Heavy users are more likely to store their telephone number (8c), school attending (8f), place of employment 8(g), and social activities (8i), than are light users. However, light users are more likely to believe that they know how their data will be shared externally by their SNS.

Privacy Policy Reader Differences

The respondents were separated into those who claim that they have read and those who admit

that they have not read their SNS privacy policy. As might be expected, there were no significant differences between these groups in any of the parts of the Data Question. However, there were highly significant differences in five of the Knowledge Questions. These results are summarized in Table 6 in Appendix C.

In all cases listed in Table 6, the respondents who did not read their SNS privacy policy were *more* likely to believe that they know what personal information is collected by their SNS (question 9), that their SNS explicitly tells them how their data will be used (question 10), that their SNS tells them if their information will be shared with internal departments (question 11), that they have a choice about how their data is used (question 14), and that they know how their information will be safeguarded (question 17).

It is a bit paradoxical that those who claim they have not read their SNS privacy policy are more willing to believe their SNS will behave regarding their personal data. Perhaps this is because those who have read the privacy policy know better!

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 4.9% store their address and 14.3% 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 28.6% store their political views, 27% store their place of employment, 35.3% store their tastes and preferences, and 36.7% 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 age, 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, school attending, and photos.

The majority of respondents (60%) 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 7 in Appendix C 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 11, 12, 13, 17, 18 and 19 have less than one-third "Yes" responses. Question 10 (does the SNS tell how personal data will be used) elicited only a 37% "Yes" response. Thus 63% of respondents 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 35% "Yes" response rate, while Question 15 (Do you have an easy way to correct your SNS data) received only a 47% response rate.

Questions 17and 18 concern security of the respondent's SNS. These questions received the lowest "Yes" response rate. Only 22% know how their information will be safeguarded (question 17) and 10% know what their site will do if there is a security breach (question 18.)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. Surprisingly, 14% of the respondents, about one in 7, leave their SNS site public (question 19). 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.

At Pace University, the required core introductory computing course contains a significant module on online privacy and security.

7. LIMITATIONS AND OPPORTUNITIES

The present study has several limitations. 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 (in responding to 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 spring 2012, 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 limitation is the restriction of the study population to one university. A broader study involving students from across the country would validate the results of the present study.

An 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 new 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 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, Mintel / 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.

Benn, S. (1971) Privacy, Freedom, and Respect for Persons. In J. Pennock and R. Chapman (Eds.), Nomos XIII: Privacy. Atherton Press, New York.

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.

Cline, J. (2010) "Privacy Training Gone Awry: Despite Good Intentions, Companies Often Make These Five Mistakes When Educating Employees about Data Protection" Computerworld, February 8, p. 24.

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.

Ho, A., Maiga, A. and Aimeur, E. (2009) "Privacy Protection Issues in Social Networking Sites" IEEE, August, pp. 273-274.

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.

Lamm, S. and Phile, R. (2009) "Still Got That Picture of Yourself Chugging a Brewski on Facebook? Better Listen to Us and Take That Pic Down! – A Look at When Social Networking Sites and Human Resource Recruiting Collide" Proceedings of the 2009 Southeastern Information for Operations Research and Management Sciences (INFORMS) Conference, Myrtle Beach, South Carolina, October 1-2, pp. 962-966.

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 Vandepeutte, 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.

Lawler, J.P. and Molluzzo, J.C. (2009) "A Study of the Perceptions of Students on Privacy and Security on Social Networking Sites (SNS) on the Internet" Proceedings of the Information Systems Education Conference (ISECON), Washington, D.C., November.

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.

Lohr, S. (2010) "Redrawing the Route to On-Line Privacy" The Sunday New York Times, February 28, p. 4.

MacMillian, D. (2009) "Facebook Banks on a Little Help from Its Friends: Mixing Its Social Network with e-Tailing Adds a Twist to On-Line Shopping – and a Source of Potential Revenue" Business Week, October 26, pp. 048-049.

MacMillian, D. (2010) "Why Facebook Wants Your ID: By Trying to Be the De Facto Standard for On-Line Identity, It's Making Privacy Advocates Nervous" Bloomberg Business Week, December 28, 2009 / January 4, 2010, pp. 092-093.

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.

Moloney, M. and Bannister, F. (2009) "A Privacy Control Theory for On-Line Environments" Proceedings of the 42nd Hawaii International Conference on System Sciences, Honolulu, Hawaii, March, p. 5.

Mooradian, N. (2009) "The Importance of Privacy Revisited" Ethics Information Technology, 11, p. 168.

Nagle, F. and Singh (2009) "Can Friends Be Trusted? Exploring Privacy in On-Line Social Networks" IEEE, Advances in Social Network Analysis and Mining, July, pp. 313-315.

Pollach,I. (2007) "What's Wrong with On-Line Privacy Policies?" Communications of the ACM, 50(9), pp. 103-108.

Prince, B. (2010) "Facebook CEO: Privacy Not the 'Social Norm'" eWEEK, January 11, p. 1.

Paullet, K.L., Rota, D.R., Turchek, J. and Swan, T. (2009) "Cyberstalking: An Exploratory Study of Law Enforcement in Allegheny County, Pennsylvania" Proceedings of the 2009 Southeastern Information for Operations Research and Management Science (INFORMS) Conference, Myrtle Beach, South Carolina, October 1-2, pp. 806-07.

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.

Rosenblum, D. (2007) "What Anyone Can Know: The Privacy Risks of Social Networking Sites" IEEE Security & Privacy, May/June, pp. 40-49.

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.

Strater, K. and Lipford, H.R. (2008) "Strategies and Struggles with Privacy in an On-Line Social Networking Community" British Computer Society, p. 117-118.

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.

Vijayan, J. (2009) "Staying on Message: How Companies Are Leveraging Social Networking Sites to Their Advantage" Computerworld, October 19, p. 26.

Westin, A. (1967) Privacy and Freedom. Atheneum Publishers, New York.

Whitcomb, K.M. and Fiedler, K.D. (2010) "The Impact of Negative Emotion on Perceived Privacy Risk in a Social Network Community" Proceedings of the Southeast Decision Sciences Institute (DSI) Conference, Wilmington, North Carolina, pp. 231-235.

Wilson, T. (2008) "Your Biggest Threat: Gen Y" Information Week, December 1, p. 20.

Zukowski, T. and Brown, I. (2007) "Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns" Communications of the ACM, October, p. 201.

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

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

_____ (2010) "A World of Connections: On-Line Social Networks Are Changing the Way People Communicate, Work and Play, and Mostly for the Better..." The Economist, January 30, p. 3.

Editor's Note:

This paper was selected for inclusion in the journal as a ISECON 2012 Meritorious Paper. The acceptance rate is typically 15% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2012.

APPENDICES

Appendix A: Figures on Social Networking Sites

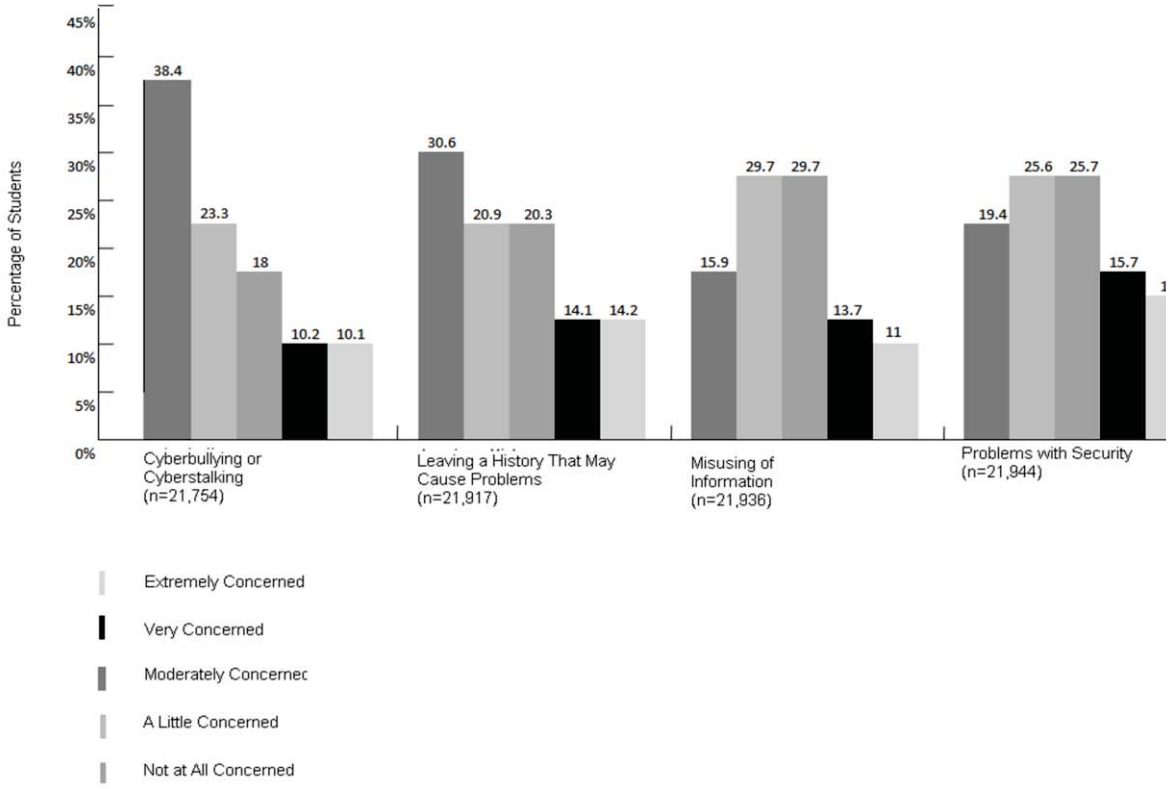

Figure 2: Social Networking Sites – Issues on Privacy and Security

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].

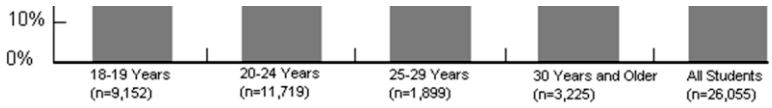

Figure 3: Social Networking Sites – Generation of Consumers (Students)

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.

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	96.2
Gender	92.2
Friends	88.4
School Attending	86.5
Photos	86.0
Age	75.2
Relationship Status	72.5
Sexual Preferences	47.4
Social Activities	43.4
Religion	36.7
Tastes and Preferences	35.3
Political Views	28.6
Place of Employment	27.0
Telephone Number	14.3
Address	4.9

Table 2 – Significant Differences Between Under and Upperclassmen

Question	p ≤ .001	p < .01	p < .05
8d		.	0.041
8f			0.050
8g	0.001		
10			0.021
14		0.005	.019
16		0.005	

Table 3 – Significant Gender Differences

Question	p < 0.01	p < 0.05	% Male	% Female
8c		0.017	19	11
8h		0.037	88	94
8k		0.034	70	79
8l		0.040	57	47
10		0.040	55	32
11		0.030	59	72
12		0.040	64	76
16	0.006		49	35

Table 4 - Significant Differences in Ethnicity

Question	p ≤ 0.050	% Caucasian	% Minority
8b	0.021	1.9	6.7
8l	0.054	55	46
9	0.029	32	46
10	0.035	60	66
11	0.023	71	63

Table 5 – Significant Differences Between Hours < 6 (Light Users) and Hours ≥ 6 (Heavy Users) Spent on SNS

Question	p ≤ .001	p < .01	p < .05	% Light	% Heavy
8c			0.050	12	21
8f			0.013	88	97
8g	0.001			23	42
8i	0.000			41	66
12		0.004		74	58

Table 6 – Significant Differences Between Readers and non-Readers of SNS Privacy Policy

Question	p ≤ .001	p < .01	% Read PP	% Not Read PP
9		0.009	30	44
10	0.000		48	73
11		0.002	57	74
14		0.003	56	76
17		0.010	69	82

Table 7 – Percent Responses to the Knowledge Questions

Question	Yes	Don't Know	No
9	61	33	6
10	37	40	23
11	31	47	23
12	27	49	24
13	27	49	24
14	35	41	24
15	47	35	17
16	61	27	12
17	22	51	27
18	10	50	41
19	14	10	76