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 Generers) 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 (Mooney 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 Vandepoelette, 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 (Aguilar, 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 (8g), 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 17 and 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


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 1: Social Networking Sites – Choices of Consumers (Students)


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


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

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

<table>
<thead>
<tr>
<th>Data Stored</th>
<th>Percent Choosing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>96.2</td>
</tr>
<tr>
<td>Gender</td>
<td>92.2</td>
</tr>
<tr>
<td>Friends</td>
<td>88.4</td>
</tr>
<tr>
<td>School Attending</td>
<td>86.5</td>
</tr>
<tr>
<td>Photos</td>
<td>86.0</td>
</tr>
<tr>
<td>Age</td>
<td>75.2</td>
</tr>
<tr>
<td>Relationship Status</td>
<td>72.5</td>
</tr>
<tr>
<td>Sexual Preferences</td>
<td>47.4</td>
</tr>
<tr>
<td>Social Activities</td>
<td>43.4</td>
</tr>
<tr>
<td>Religion</td>
<td>36.7</td>
</tr>
<tr>
<td>Tastes and Preferences</td>
<td>35.3</td>
</tr>
<tr>
<td>Political Views</td>
<td>28.6</td>
</tr>
<tr>
<td>Place of Employment</td>
<td>27.0</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>14.3</td>
</tr>
<tr>
<td>Address</td>
<td>4.9</td>
</tr>
</tbody>
</table>

#### Table 2 – Significant Differences Between Under and Upperclassmen

<table>
<thead>
<tr>
<th>Question</th>
<th>p ≤ .001</th>
<th>p &lt; .01</th>
<th>p &lt; .05</th>
</tr>
</thead>
<tbody>
<tr>
<td>8d</td>
<td></td>
<td></td>
<td>0.041</td>
</tr>
<tr>
<td>8f</td>
<td>0.001</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0.005</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>0.005</td>
<td></td>
<td>.019</td>
</tr>
<tr>
<td>16</td>
<td>0.005</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Table 3 – Significant Gender Differences

<table>
<thead>
<tr>
<th>Question</th>
<th>p &lt; 0.01</th>
<th>p &lt; 0.05</th>
<th>% Male</th>
<th>% Female</th>
</tr>
</thead>
<tbody>
<tr>
<td>8c</td>
<td>0.017</td>
<td>0.037</td>
<td>19</td>
<td>94</td>
</tr>
<tr>
<td>8h</td>
<td>0.034</td>
<td>0.040</td>
<td>70</td>
<td>79</td>
</tr>
<tr>
<td>8k</td>
<td>0.040</td>
<td>0.030</td>
<td>57</td>
<td>72</td>
</tr>
<tr>
<td>10</td>
<td>0.040</td>
<td>0.040</td>
<td>55</td>
<td>72</td>
</tr>
<tr>
<td>11</td>
<td>0.030</td>
<td>0.040</td>
<td>59</td>
<td>76</td>
</tr>
<tr>
<td>12</td>
<td>0.040</td>
<td>0.040</td>
<td>64</td>
<td>76</td>
</tr>
<tr>
<td>16</td>
<td>0.006</td>
<td></td>
<td>49</td>
<td>35</td>
</tr>
</tbody>
</table>

#### Table 4 - Significant Differences in Ethnicity

<table>
<thead>
<tr>
<th>Question</th>
<th>p ≤ .050</th>
<th>% Caucasian</th>
<th>% Minority</th>
</tr>
</thead>
<tbody>
<tr>
<td>8b</td>
<td>0.021</td>
<td>1.9</td>
<td>6.7</td>
</tr>
<tr>
<td>8f</td>
<td>0.054</td>
<td>55</td>
<td>46</td>
</tr>
<tr>
<td>9</td>
<td>0.029</td>
<td>32</td>
<td>46</td>
</tr>
<tr>
<td>10</td>
<td>0.035</td>
<td>60</td>
<td>66</td>
</tr>
<tr>
<td>11</td>
<td>0.023</td>
<td>71</td>
<td>63</td>
</tr>
</tbody>
</table>
Table 5 – Significant Differences Between Hours < 6 (Light Users) and Hours ≥ 6 (Heavy Users) Spent on SNS

<table>
<thead>
<tr>
<th>Question</th>
<th>p ≤ .001</th>
<th>p &lt; .01</th>
<th>p &lt; .05</th>
<th>% Light</th>
<th>% Heavy</th>
</tr>
</thead>
<tbody>
<tr>
<td>8c</td>
<td></td>
<td>0.050</td>
<td></td>
<td>12</td>
<td>21</td>
</tr>
<tr>
<td>8f</td>
<td></td>
<td>0.013</td>
<td></td>
<td>88</td>
<td>97</td>
</tr>
<tr>
<td>8g</td>
<td>0.001</td>
<td></td>
<td></td>
<td>23</td>
<td>42</td>
</tr>
<tr>
<td>8i</td>
<td>0.000</td>
<td></td>
<td></td>
<td>41</td>
<td>66</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>0.004</td>
<td></td>
<td>74</td>
<td>58</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Question</th>
<th>p ≤ .001</th>
<th>p &lt; .01</th>
<th>% Read PP</th>
<th>% Not Read PP</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td></td>
<td>0.009</td>
<td>30</td>
<td>44</td>
</tr>
<tr>
<td>10</td>
<td>0.000</td>
<td></td>
<td>48</td>
<td>73</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>0.002</td>
<td>57</td>
<td>74</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>0.003</td>
<td>56</td>
<td>76</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>0.010</td>
<td>69</td>
<td>82</td>
</tr>
</tbody>
</table>

Table 7 – Percent Responses to the Knowledge Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>Don’t Know</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>61</td>
<td>33</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>37</td>
<td>40</td>
<td>23</td>
</tr>
<tr>
<td>11</td>
<td>31</td>
<td>47</td>
<td>23</td>
</tr>
<tr>
<td>12</td>
<td>27</td>
<td>49</td>
<td>24</td>
</tr>
<tr>
<td>13</td>
<td>27</td>
<td>49</td>
<td>24</td>
</tr>
<tr>
<td>14</td>
<td>35</td>
<td>41</td>
<td>24</td>
</tr>
<tr>
<td>15</td>
<td>47</td>
<td>35</td>
<td>17</td>
</tr>
<tr>
<td>16</td>
<td>61</td>
<td>27</td>
<td>12</td>
</tr>
<tr>
<td>17</td>
<td>22</td>
<td>51</td>
<td>27</td>
</tr>
<tr>
<td>18</td>
<td>10</td>
<td>50</td>
<td>41</td>
</tr>
<tr>
<td>19</td>
<td>14</td>
<td>10</td>
<td>76</td>
</tr>
</tbody>
</table>