Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook

Alyson L. Young
The University of Western Ontario
Master of Arts in Media Studies
London, Ontario, Canada N6A 5B7
ayoung82@email.com

Anabel Quan-Haase
The University of Western Ontario
Faculty of Information and Media Studies
Department of Sociology
London, Ontario, Canada N6A 5B7
aquan@uwo.ca

ABSTRACT

Despite concerns raised about the disclosure of personal information on social network sites, research has demonstrated that users continue to disclose personal information. The present study employs surveys and interviews to examine the factors that influence university students to disclose personal information on Facebook. Moreover, we study the strategies students have developed to protect themselves against privacy threats. The results show that personal network size was positively associated with information revelation, no association was found between concern about unwanted audiences and information revelation and finally, students' Internet privacy concerns and information revelation were negatively associated. The privacy protection strategies employed most often were the exclusion of personal information, the use of private email messages, and altering the default privacy settings. Based on our findings, we propose a model of information revelation and draw conclusions for theories of identity expression.

Categories and Subject Descriptors

K.4.1 [**Computers and Society**]: Public Policy Issues – *privacy.*

General Terms

Human Factors, Security.

Keywords

Social Network Sites (SNSs), Facebook, Information Revelation, Internet Privacy, Privacy Protection Strategies.

1. INTRODUCTION

Social network sites (SNSs) have become increasingly popular, with an estimated 80 to 90 per cent of undergraduate students actively participating in such services as MySpace, Friendster and Facebook [Strater and Richter 2007]. What attracts students to SNSs is their ability to converse with friends, share digital cultural artifacts and ideas, and connect to vast networks of people [boyd and Heer 2006]. Despite these potential benefits, scholars, privacy advocates and the media have raised concerns about the risks associated with the disclosure of personal information on SNSs [Barnes 2006; Govani and Pashely 2005; Gross & Acquisti 2005].

Much of the debate has focused on *information revelation*, that is, the amount and type of information users disclose [Govani and Pashely 2005; Gross and Acquisti 2005]. Consistently, research has found that users disclose accurate personal information on their profiles, seemingly without much concern. Gross and Acquisti (2005) argue that in disclosing personal information on SNSs users effectively place themselves at a greater risk for cyber and physical stalking, identity theft and surveillance. However, the reasons why users willingly disclose information on their profiles have not been sufficiently investigated. An important study aimed at addressing this research question found that three important factors influence information revelation: future audiences, general privacy concerns, and gender [Tufekci 2008]. To further investigate privacy in SNSs, we continue Tufekci's line of inquiry and investigate additional factors that could influence information revelation.

Our study also expands on the current literature by examining students' privacy protection strategies on Facebook. While several studies have demonstrated self-disclosure practices in university students and the threats associated with information revelation, little is known about the strategies students employ to protect themselves from privacy threats. We argue that these strategies could serve as moderating factors alleviating some of the problems that might emerge from information revelation. This portrays students as active participants in the construction of their identity, and not only as naïve users.

2. UNIVERSITY STUDENTS' INFORMATION REVELATION ON FACEBOOK

University students are heavy users of Facebook. Indeed, Lampe et al. [2006] found that 70 per cent of students report spending thirty minutes or less on Facebook per day and 21 per cent indicate spending more than an hour a day on average using the site. Research has also shown that students tend to disclose personal information on their profiles [Govani and Pashley 2005; Gross and Acquisti 2005; Tufekci 2008]. For example, Gross and Acquisti [2005] found that 82 per cent of active Facebook users disclosed personal information such as their birth date, cell phone number, personal address, political and sexual orientation, and partner's name. Tufekci [2008] has suggested that many students see a certain degree of information revelation as necessary to make SNSs useful: 'why have a profile if your profile doesn't say enough about who you are?' [p. 33; see also Acquisti & Gross 2005]. Based on this previous research, we expect that students'

C&T'09, June 25-27, 2009, University Park, Pennsylvania, USA.
ACM 978-1-60558-601-4/09/06

frequency of Facebook use will correlate with their disclosure of personal information on Facebook. That is, the more often students log into their Facebook accounts, the more information they would be likely to reveal. For this reason, we propose the following hypothesis:

Hypothesis 1: Frequency of Facebook use will be positively associated with information revelation on Facebook.

Jenny Sundén [2003] argues that in order for individuals to exist online they must first write themselves into being. In SNSs, such as Facebook, the process of writing oneself into existence occurs through the construction of a profile, which reveals personal information about the user. Lampe et al. [2007] suggest that the inclusion of profile elements, such as a self-description, a statement of relationship status, a description of one's interests, and a photograph of oneself, enables users to signal aspects of their identity, which assist other users in making decisions about declaring friendship links. They also argue that the ability to search SNS profiles reduces the amount of time spent locating former high school friends, current classmates, or people located in the same university or college dormitory. Furthermore, research has shown that users with larger social networks are often more forthcoming and open with their personal information on these sites. For example, Jones and Soltren [2005] revealed that users with more than three hundred friends disclosed more information concerning their interests (85.3 per cent compared to 64.1 per cent), favorite music (82.9 per cent compared to 64 per cent), and clubs (81 per cent compared to 51.5 per cent) than users with comparably smaller social networks. Hence, it should be expected that the more profile elements included on a user's profile, the easier and more accurate a search will be, and the more likely that friendship connections will occur. For this reason, we explore the relationship between network size and information revelation on Facebook. This leads to the following hypothesis:

Hypothesis 2: Facebook personal network size will be positively associated with information revelation on Facebook.

Research has demonstrated that general concern for Internet privacy has an effect on the information revelation behaviors of Internet users [Pew 2000; Viseu et al. 2003]. A 2000 Pew Internet survey reports that out of 45 per cent of individuals who have not provided real personal information to access a Web site, 61 per cent identify themselves as 'hard-core privacy defenders.' These individuals refuse to provide personal information to use an Internet site because they believe that Internet tracking is harmful, that their online activities are not private, and that there is a need to be concerned about businesses obtaining their personal information. Research has also suggested that individuals with a comparably low level of concern for Internet privacy tend to be much more forthcoming and open with the disclosure of their personal information online. Viseu et al. [2003] found that online users who believe that privacy is only a concern once it has been lost or breached were inclined to perceive the benefits of disclosing personal information in order to use an Internet site as greater than the potential privacy risks. Furthermore, Joinson et al. [in press], in their study examining privacy, trust and self-disclosure online found that trust and perceived privacy had a strong affect on individuals' willingness to disclose personal information to a web site. They also indicate that individuals' trust in the privacy threat – that is, the likelihood that a privacy breach will occur – influences their information revelation decisions. In other words, if the individual does not think their information will be used for potentially harmful purposes, they are more likely to disclose personal information online. Based on these prior findings, we propose the following hypothesis:

Hypothesis 3: Concern for Internet privacy will be negatively associated with information revelation on Facebook.

The literature on privacy online has suggested that Internet users are generally concerned about unwanted audiences obtaining personal information. Fox et al. [2000], report that 86 per cent of Internet users are concerned that unwanted audiences will obtain information about them or their families, 70 per cent are concerned that hackers will access their credit card information, and 60 per cent are concerned that someone will find out personal information from their online activities. Acquisti and Gross [2006] found similar results, showing that students expressed high levels of concern for general privacy issues on Facebook, such as a stranger finding out where they live and the location and schedule of their classes, and a stranger learning their sexual orientation, name of their current partner, and their political affiliations.

Despite these concerns, research has also shown that users continue to disclose personal information and often disclose accurate personal information online [Acquisti and Gross 2006; Govani and Pashley 2005; Gross an Acquisti 2005; Pew 2000; Tufekci 2008; Viseu et al. 2003]. In their examination of information sharing and privacy on Facebook, Acquisti and Gross [2006] revealed that 89 per cent of students used their full name on their profiles, 87.7 per cent had disclosed their birth date and 50.8 per cent had listed their current address. Tufekci [2008] found that concern about unwanted audiences had an impact on whether or not students revealed their real name in MySpace and whether or not students revealed their religious affiliation on MySpace and Facebook. Therefore, there may be an association between an individual's concern about unwanted audiences accessing his or her profile and the amount and types of information he or she chooses to reveal on Facebook. Therefore, we predict that:

Hypothesis 4: Concern for unwanted audiences will be negatively associated with information revelation on Facebook.

Another way to examine students' information revelation on Facebook is by looking at the concept of profile visibility. Profile visibility refers to the extent to which users' profiles are accessible by other Facebook users. Typically, SNSs allow users to alter the visibility of their profiles in order to restrict unwanted or unknown others from accessing their profile and viewing their personal information. On Facebook, users can set their profile to one of four visibility levels: 'all networks and all friends', 'some networks and all friends', 'friends-of-friends', and 'only friends'. While no research has examined the relationship between profile visibility and information revelation, it seems likely that the more visible the user's profile, the less information he or she will reveal on Facebook. That is, we expect that users with restricted profiles would be more inclined to reveal personal information on Facebook than users with open profiles, as their information would be protected against possible invasions. For this reason, we propose the following hypothesis:

Hypothesis 5: Profile visibility will be negatively associated with information revelation on Facebook.

3. UNIVERSITY STUDENTS' PRIVACY PROTECTION STRATEGIES ON FACEBOOK

Users actively construct their identity on SNSs through the disclosure of personal information [boyd 2008]. However, research suggests that students are not completely naïve in their disclosure practices. boyd (in press) found that teens frequently falsify personally identifiable information, such as their name, location, and age, in order to protect themselves against privacy concerns on MySpace. Similarly, in her examination of MySpace and Facebook, Tufekci [2008] found that students' concern for unwanted audiences accessing their profiles influenced them to use protective measures, such as altering the visibility of their profiles to 'only friends' on Facebook and using nicknames or monikors in place of real names on MySpace. In terms of the privacy protection strategies employed by students, previous research on privacy in SNSs has found conflicting evidence as to whether or not users employ tactics to protect themselves against privacy threats on SNSs. In two separate studies conducted at Carnegie Mellon University (CMU), for instance, Govani and Pashley (2006) and Gross and Acquisti (2005) found that despite awareness and concern for Internet privacy, users seldom provide false information and very rarely alter their privacy settings. While much of the debate in the literature has focused on the threats, the strategies have been largely ignored. To fill this gap, the present study investigates the following exploratory research question:

What strategies do undergraduate students employ to protect themselves against privacy threats on Facebook?

4. METHODS

4.1 Participants

Participants were undergraduate university students from a large, research-intensive university in English Canada enrolled in communication studies. The final survey sample consisted of 77 respondents with a mean age of 19.68 (*S.D.*=1.26), ranging from 17–25 years. Seventy-one per cent of respondents were female, which is 13.7 per cent higher than the proportion of female university students in Canada in the 2005–2006 academic year [Statistics Canada 2005], but representative of the proportion of female students enrolled in communication studies at the university under study in the 2006–2007 academic year. The interview sample consisted of 21 undergraduate students, of which 16 were female.

4.2 Procedures

Ethics approval was obtained prior to commencing the study. Participation was voluntary. Participants for the survey were recruited from two communication studies courses. Eighty-five students completed a paper-and-pencil questionnaire. Eight students identified themselves as non-Facebook users and were removed from the final sample. Participants for the interviews were recruited through posters, which were displayed on bulletin boards across campus. Nineteen respondents participated in a face-to-face interview and two respondents opted for an email-based interview. All interviews conducted face-to-face were recorded and transcribed with participants' consent. During the interviews a profile analysis was conducted, which consisted of asking students to log on to Facebook and discuss the information they have revealed, the privacy settings they have in place and the protective strategies they employ. This provided rich accounts from the respondents to expand and elaborate on the information already obtained from surveys and interviews. The profile analysis also showed that students are often unaware or have forgotten what information they have disclosed and what privacy settings they have activated. By discussing the profiles in the presence of students, rather than downloading profiles or only relying on questionnaires [Govani and Pashley 2005; Gross and Acquisti 2005], we gain a better understanding of information revelation and privacy practices. Moreover, it allowed us to discuss what information is accurate, why certain types of information were posted and not others, and the social meaning of the information included on the profile. Data collection took place between October 2007 and February 2008.

4.3 Measures

4.3.1 Information Revelation

To investigate respondents' information revelation, a scale adopted from Govani and Pashley [2005] was used. Additional items were added to include a larger set of information types and to assess the extent to which respondents reveal information on Facebook (see Figure 1). Respondents were asked to report which of several salient elements (such as relationship status, e-mail address, and cellular phone number) they included on their Facebook profile. Based on the items, an additive scale was created that ranged from 1–17 and measured the number of 'yes' responses to the seventeen types of information that could be revealed. These items offer insight into the degree to which respondents reveal personal information on Facebook.

4.3.2 Frequency of Facebook Use

The frequency of Facebook usage was measured asking respondents to report how often they visit Facebook. Respondents reported their frequency of use on an eight-point scale (8='several times a day'; 7='once a day'; 6='several times a week'; 5='once a week'; 4='several times a month'; 3='once a month'; 2='a couple of times a year'; 1='never').

4.3.3 Personal Network Size

Respondents were asked to report their total number of Facebook friends: 'Approximately, how many Facebook friends do you have?' This was used as a measure of personal network size on Facebook.

4.3.4 Concern for Internet Privacy

This measure was adopted from Tufekci [2008] and was used to assess the extent to which respondents are concerned about general Internet privacy: 'How concerned are you, if at all, about Internet privacy?' Respondents were asked to indicate their level of concern: 1='not concerned at all'; 2='not too concerned'; 3='somewhat concerned'; 4='very concerned'.

4.3.5 Concern about Unwanted Audiences

Based on Tufekci's [2008] analysis of future audiences, seven items were employed to measure respondents' concern about profile access by unwanted audiences (such as current or future employers, university administrators, and corporations). The items were measured on a five-point Likert scale (1='strongly disagree' and 5='strongly agree'). Based on the items, an additive scale was created that measured respondents' concern about unwanted audiences accessing their profile. These items formed a reliable scale with Cronbach's alpha 0.84 (*M* =3.02; *SD* =.13). The scale measured the degree to which respondents believe that unwanted audiences might access their profiles (see Table 2).

4.3.6 Profile Visibility

Profile visibility was measured using a scale adopted from the 'Pew social networking websites and teens survey' [2007], which assessed the extent to which respondents' profiles are accessible by other Facebook users. The profile visibility levels were coded as 1='visible to only my friends'; 2='visible to some of my networks and all of my friends'; 3='visible to all of my networks and all of my friends'; 4='visible to anyone searching Facebook'. Table 1 provides the means and standard deviations for key measures employed in this study.

Table 1. Means and standard deviations of key measures

	M	***S.D.***
Information Revelation	10.47	1.97
Frequency of Facebook Use	3.8	3.89
Personal Network Size	401.62	198.64
Concern for Internet Privacy	2.92	0.74
Concern about Unwanted Audiences	18.17	5.70
Profile Visibility	3.47	1.08

4.3.7 Privacy Protection Strategies

To investigate respondents' tactics for negotiating privacy on Facebook, a series of attitudinal questions were formulated. The items included in this measure were designed to tap the extent to which respondents use self-censorship tactics (such as excluding personal information) and other privacy protection strategies (such as sending private emails instead of using the wall to post messages) to protect themselves against privacy threats while using Facebook. The answers to these questions were reported on a 5-point Likert scale (1="strongly disagree"; 2="disagree"; 3="neither disagree nor agree"; 4=agree; 5="strongly agree"). See Table 3 for item wording, means and standard deviations.

4.4 Data Analysis

We ran a hierarchical regression analysis to examine the influence of Facebook usage, personal network size, concern for Internet privacy, concern about unwanted audiences and profile visibility in predicting information revelation. To analyze the qualitative data, we used the framework-based approach proposed by Ritchie et al. [2003], which consists of classifying and organizing the data into a thematic framework based on key themes, concepts and categories. The main themes were then subdivided into a succession of related subtopics and the data from each respondent were synthesized and placed under the appropriate subtopic of the thematic framework.

5. RESULTS

5.1 Information Revelation

In line with previous research [Govani and Pashley 2005; Gross and Acquisti 2005; Tufekci 2008], the data show high levels of information revelation on Facebook. An overwhelming 99.35 per cent reported using their actual name in their profile (first and last name). Nearly two-thirds of respondents indicated their sexual orientation, relationship status, and interests (such as favorite books, movies and activities). Large percentages of respondents noted their school name (97.4 per cent), e-mail address (83.1 per cent), birth date (92.2 per cent), the current city or town in which they live (80.5 per cent), and almost all respondents reported posting an image of themselves (98.7 per cent) and photos of their friends (96.1 per cent). By contrast, few respondents reported disclosing their physical address (7.9 per cent), their cell phone number (10.5 per cent) or their IM screen name (16 per cent), thereby limiting the likelihood of individuals contacting or locating them outside of Facebook.

Figure 1 shows the information indicated on respondents' profiles by gender. For the most part, the data show that there was very little difference in terms of the types of information that female and male respondents include on their profiles. For instance, female and male students were as likely to disclose their school name (96.4 per cent compared to 100 per cent), email address (85.5 per cent compared to 85 per cent), relationship status (64.8 per cent compared to 60 per cent) and birth date (94.5 per cent compared to 95 per cent). The only items that showed differences were current address, $\chi2(1, N = 72) = 5.47, p < .05$, and political views, $\chi2(1, N = 72) = 13.29, p > .05$, with females indicating these types of information less than males.

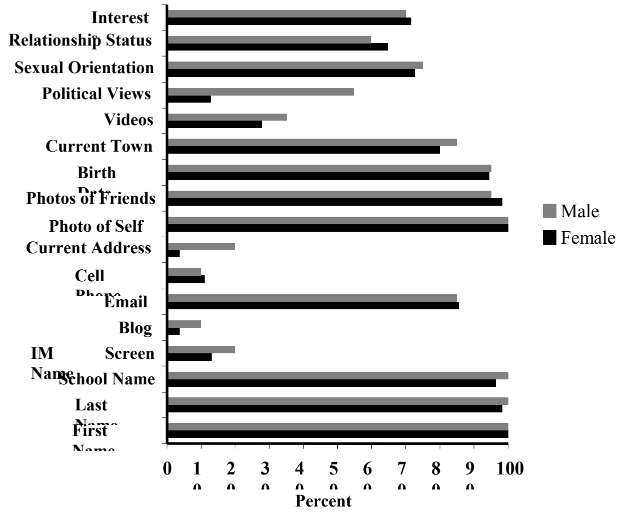

Figure 1. Information on profile by gender

Sixty-four per cent of respondents had adjusted the visibility of their profile to 'only friends', thereby restricting profile access from unwanted or unknown individuals, while only 7.9 per cent had opted to leave their profile open to 'anyone' searching the Facebook network. The data also reveal that nearly a quarter of respondents chose to either leave their profiles open to 'all networks and all friends' (14.5 per cent) or 'some networks and all friends" (6.6 per cent), thus affording all individuals within their designated networks access to their profiles.

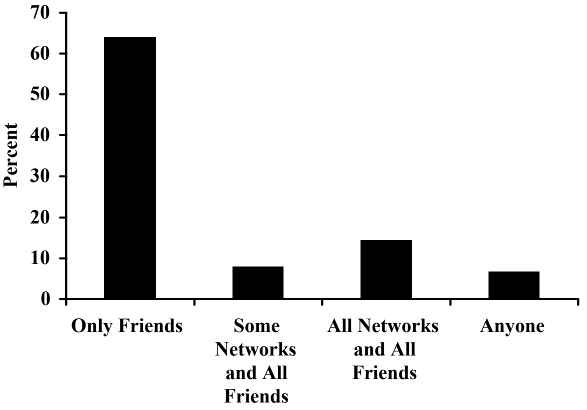

Figure 2. Profile visibility

The items on unwanted audiences show that users have a concern about unwanted audiences. Unwanted audiences refer to those individuals not directly linked to the SNS user who may gain access to a user's profile without his or her knowledge or consent. The concern is highest for the following groups gaining access to private data: political parties, sexual predators, employers and university administrators.

Table 2: Concern about unwanted audiences items

Individual Items	*M*	*S.D.*
Future employers will use the personal information contained on my Facebook site to assess my suitability with their company	3.15	1.31
University admissions officers have started using the personal information on Facebook sites to assess applicant suitability prior to offering admissions	2.52	1.19
Police officers are using Facebook to track underage drinking and other illegal activities	2.98	1.40
Universities are monitoring Facebook postings, personal information and images to identify university code violators (i.e., involvement in illegal activities)	3.05	1.31
Employers are using Facebook to monitor the extra-curricular activities of their employees	3.02	1.24
Sexual predators use social network sites such as Facebook to track, monitor and locate potential victims	3.57	1.26
Political parties have begun using Facebook to target young professionals and students through the use of advertisements and data mining	3.66	1.21

1="strongly disagree"; 2="disagree"; 3="neither disagree nor agree"; 4="agree"; and, 5="strongly agree"

5.2 Information Revelation Model

Model 1 shows no association between frequency of Facebook use and information revelation providing no support for Hypothesis 1. There was support for Hypothesis 2: personal network size was positively associated with information revelation. The larger students' personal network on Facebook, the more likely they were to reveal information. In the second block, we tested hypotheses 3 and 4 by entering the two concern variables into the model. While general concern for Internet privacy was negatively associated with information revelation, concern for unwanted audiences showed no association with information revelation. In the last block, we tested hypothesis 5 by entering profile visibility into the model. Profile visibility was positively associated with information revelation. The final model accounted for 40 per cent of the variance in information revelation. Table 2 provides the OLS regression predicting frequency of use and profile update. [1]

Table 3. OLS regression predicting frequency of use and profile update

	Information Revelation			
	Model 1	Model 2	Model 3	Model 4
Frequency of Facebook use	.153	.142	.143	.190
Personal network size	.388**	.508**	.509***	.502***
Concern for Internet privacy		-.488***	-.439***	-.399***
Concern about unwanted audiences			-.040	-.019
Profile visibility				.269**
Change in Adjusted R^2	.192	.187	.001	.068
Final Adjusted R^2	.167	.349	.341	.403

*p<.05; **p<.01; ***p<.001

5.3 Interview Data

5.3.1 Information Revelation on Facebook

Interviews conducted as part of the study revealed that the profile fields populated most often by students consist of basic personal information: twenty of 21 interviewees included their full name, sex, and an accurate or semi-concealed image, and 15 of 21 included their birth date. The primary reason was to assist their friends and peers in locating them when conducting searches on Facebook. As one respondent, Melanie, a 20-year-old social

[1] We test the effect of gender in two separate models. The results are reported online: http://publish.uwo.ca/~aquanhaa/.

science student, notes in reference to her decision to disclose an accurate profile image: “It just makes it easier for [friends] if they want to search for me on Facebook, they know this is the right person.” By contrast, contact information was by far the least populated profile section: all 21 interviewees excluded their physical address and landline phone number, and 18 of 21 chose to exclude their cell phone number. Several interview respondents mentioned that their decision to exclude this type of information was to reduce their chances of unwanted contact or physical harm from unknown others. For example, Justine, a 20-year-old science student, states: “I don’t want strangers knowing what my phone number is and then look me up and find out where I live.” Hence, they did not mind having their personal information on the Internet, but a link between the digital and their whereabouts in the physical world was something most felt uncomfortable about.

The interview data also provide insight into why students use Facebook and the benefits they derive from its use, which may further assist in understanding their information revelation behaviors on the site. The first theme identified was the desire to stay in touch with friends nearby and faraway. Diana, a 25-year-old health science major, reports using Facebook to maintain contact with geographically distant friends. Facebook allows her to find out information about her friends’ activities without a significant time commitment. The second theme identified was to receive up-to-date information on social events. Several respondents noted that students are increasingly using Facebook to meet, and that it is often the only place to find out about events. Ashley, a first year medical student, reports using Facebook almost exclusively for this purpose, stating that Facebook membership is required to gain access to this type of information.

The third theme identified by the interview respondents was photograph access and/or storage. Facebook allows users to create digital photo albums, providing an easy and convenient way to store and organize pictures from events, activities, locations, etc. Samantha, a second year music major, reports that her Facebook profile is comprised mainly of albums from camp and various childhood and adolescent events. Sharing digital content hence is a primary activity on Facebook for this user group. A fourth theme identified by respondents was the use of Facebook as a replacement for email and/or instant messaging. For example, Elizabeth, a 24-year-old medical student, reports that she uses Facebook instead of email to send quick messages to friends. Users find it convenient as they can access Facebook from anywhere and do not have to look up email addresses or phone numbers. Facebook in this regard functions as an address book that is kept and updated by its users.

An additional theme that emerged in the interviews was whether or not the information had been previously mentioned in an offline context. For example, Charlie, a 23-year-old science student, noted, “What is important is not putting up things that I would under normal circumstances conceal, such as personal matters of finance, job status, where I live … stuff like that. I suppose the influence then is my own judgment and not external.” Similarly, Andrew, a 20-year-old music major, reported that his decision to either reveal or conceal personal information on Facebook was influenced by whether or not he had previously discussed the information with friends outside of Facebook. Only if the information had been revealed offline, did he subsequently reveal it on Facebook. Thus, the experiences of Charlie, Andrew and others suggest that information deemed too personal to reveal offline, is also too personal to reveal on Facebook and therefore is excluded from the students’ profile.

5.3.2 Privacy Concerns on Facebook

In the interviews, respondents also mentioned three key types of concern that impacted their information revelation on Facebook. The first concern was that their information would be used for potentially harmful purposes by unknown others. For example, Rebecca, a 22-year-old humanities student, states: ‘I guess just someone being able to know where I am based, on finding my face on Facebook. I don’t want people to be able to find me.’ To address her concerns, Rebecca has chosen to exclude her landline phone number and physical address from her profile, and has falsified the name of her hometown, using in its place ‘Boonies, Ontario’. The second concern mentioned by respondents was that their information would be used, sold or appropriated without their knowledge or consent. Three of 21 interviewees mentioned data mining as a primary concern. For example, Melinda a 25-year-old humanities student notes: “I’m concerned with the fact that they own everything that you put on there. I would say that is my biggest concern. I think that’s highly unethical personally …. I don’t want people profiting from my demographics.” To protect herself against data mining on Facebook, Melinda reports that she does not disclose anything on the site that someone wouldn’t be able to find somewhere else. Finally, the last concern reported by respondents was that known others—that is, individuals known to the user in an offline context—would see information and/or images posted on Facebook that was not intended for them to view. For example Tara, a 4th year social science major, explains that she is concerned with individuals from high school learning more about her than she would normally be willing to discuss. To address her privacy concerns, Tara has blocked her profile and her tagged photos, as well as restricted non-Facebook friends from viewing her Friends List.

For the most part, students’ information revelation was influenced by negative reports in the media rather than personal experience. However, personal experience also influenced students’ behaviors. Two students in the interview sample did report explicit events that affected their information revelation behavior on the site. Brian, a first-year communication studies student, for example, indicated that while in high school he faced expulsion for his involvement in a Facebook group. Brian reports that after the event, the first thing he did was modify his privacy settings. He also reported that the incident has made him much more cautious about the images tagged of him on Facebook, stating that he either untags or asks for images to be removed from the site. Furthermore, the incident has affected the types of messages he posts to friends’ walls. He states: “everything I type on a wall I make sure ... who am I saying it to? If someone were to read this, what would they think? I stay away from profanity now.” Finally, Brian’s experience has also influenced his decision to join groups and accept invites to events. “I don’t accept every group as well as events. If I get an invitation, even if I will be going, I don’t respond unless it’s an event that I trust. You second guess everything you do now.”

5.3.3 Privacy Protection Strategies on Facebook

Based on negative media accounts or their own negative experience with the site, users have developed strategies to protect their privacy. We found that students employ a wide range of strategies and that each strategy has unique characteristics.

Table 4 shows that the most commonly used strategies were 1) to send private email messages instead of posting messages to a friend's wall, 2) to change the default privacy settings, and 3) to exclude personal information. Other important strategies include untagging oneself from images, deleting messages posted to one's Facebook wall, and limiting access to one's profile. Blocking users and providing fake or inaccurate information are less frequently employed strategies.

Table 4. Privacy Protection Strategies

Individual Items	***M***	***S.D***
I have provided fake or inaccurate information on Facebook to restrict people I don't know from gaining information about me	1.66	1.03
I have excluded personal information on Facebook to restrict people I don't know from gaining information about myself	4.08	1.17
I have sent private email messages within Facebook instead of posting messages to a friend's wall to restrict others from reading them message	4.72	0.68
I have blocked former contacts from contacting me and accessing my Facebook profile	2.91	1.71
Certain contacts on my Facebook site only have access to my limited profile	3.47	1.70
I have changed my default privacy settings activated by Facebook	4.33	1.25
I have deleted messages posted to my Facebook wall to restrict others from viewing/reading the message	3.64	1.55
I have untagged myself from images and/or videos posted by my contacts	3.85	1.55

Scale: 1="strongly disagree"; 2="disagree"; 3="neither disagree nor agree"; 4=agree; 5="strongly agree".

Based on an analysis of the interview data, we discovered that strategies served different privacy objectives. These privacy objectives can be described in terms of Goldie's categorization of privacy concerns. Goldie [2006] describes expressive privacy concerns as the ability to control the extent to which an individual is known by chosen others. By contrast, an informational privacy concern is defined as the right to control access to one's personal information [see also DeCew 1997; Weston 1972]. An expressive privacy concern, for example, is that certain individuals known to the Facebook user in an offline context will stumble on their posting, images, or information. As one respondent, Christine, a first year business student, explains: "I have a lot of family members on my Facebook account and, I mean, they don't want to see everything that goes on it. So, when someone tags a picture of me and I'm not comfortable with it, I'll untag it and ask them to remove it altogether. I've had one [negative] experience with one family member who did come across a picture and it was 'bad news.' So, I try to do that [untag and remove photos] for the most part." From this comment, two things are apparent. First, the respondent is aware of the expressive privacy risks associated with the disclosure of personal information and images on Facebook. Second, she has enacted measures to protect herself against subsequent negative feedback from her family. In other words, the respondent has opted to limit her self-expression in order to reduce the likelihood of family members accessing specific content.

Use of the limited profile was another measure employed by respondents to protect their expressive privacy. The limited profile allows users to restrict certain groups from accessing various information types. Justine, a third year science student, for example, reported placing her sister and their mutual friends on a limited profile to restrict them from accessing information that could subsequently be used to inform her mother of her activities. In this way, the limited profile enables Justine and others to protect their expressive privacy without significantly limiting their self-expression and freedom to associate.

Despite the mention of expressive privacy concerns, it was the informational privacy concerns that respondents faced when using Facebook that appeared the most pressing and the most in need of protection. An informational privacy concern, for example, is that unwanted audiences will access information and use it for potentially harmful purposes. Rebecca, a 22-year-old humanities student, for instance, explains: "I guess [I am concerned with] someone just being able to know where I am based on just finding my face on Facebook. I don't want people to be able to find me." To address her informational privacy concerns, Rebecca has enacted a variety of protective measures including altering her profile visibility, using a semi-concealed profile image, and excluding contact information. Similar comments around concerns about unwanted audiences came from the majority of respondents, and most employed a combination of the strategies used by Rebecca.

It is interesting to note that students do not use fake or inaccurate information as a protective measure. The primary reason expressed by our sample was that it seemed nonsensical to falsify information because their friends would question the validity of the information disclosed. A few respondents also noted that their disclosure of false information in the past had caused confusion, resulting in numerous messages being sent to inquire about the validity of the information. While the majority of respondents opted to include only valid information, a few respondents noted that their 'about me' section was in fact fictional. These respondents indicated that the informational was intended to be comical rather than intentionally deceitful. These results are consistent with previous research, which has found that SNS profiles tend to be either honest and truthful or playful and ironic, instead of intentionally deceitful [Donath and boyd 2004; Lampe, Ellison, and Steinfield 2007].

6. DISCUSSION

In the present study, we address three issues of importance to the privacy and SNSs literature. First, we investigate the reasons why users reveal personal information on SNSs and propose a preliminary model. Second, we describe a novel method of data collection that includes profile analysis as a means to both corroborate data obtained from self-reports and elicit further descriptions from participants. Facebook is particularly well-suited for this type of data collection as profiles are identical for all users allowing for easy comparison across participants. Third, we propose that examining privacy protection strategies is essential as these represent an important component of information revelation. Examining information revelation in isolation does not provide a complete picture of users' understanding of privacy. Privacy protection strategies show users' reaction to privacy concerns and their active engagement with the information they choose to reveal on SNSs.

The SNSs literature has extensively investigated the information revelation practices of students. We continue this line of research by investigating the reasons why students reveal information on these sites. Our preliminary model shows three factors associated with information revelation. We found that the larger students' Facebook network size, the more information is revealed in their profiles. In accord with Lampe et al. [2007], we find that profile elements act as signals, revealing aspects of a user's personality. Through these signals users establish *common ground* and make decisions about declaring friendship connections. Information revelation seems to serve a social purpose increasing students' opportunities for social interaction and participation, as well as for the maintenance and formation of relationships [donath and boyd 2004].

Concern for Internet privacy was negatively associated with users' information revelation practices. That is, students with a high level of concern for Internet privacy tended to disclose less personal information on Facebook. Contrary to previous findings, our results suggest that students not only 'say they are concerned' about privacy on the Internet, they also make a concerted effort to protect themselves against possible invasions by withholding personal information on their profiles. By contrast, we did not find an association between concern about unwanted audiences and information revelation on Facebook: students' concern about unwanted audiences did not impact the amount of information that they chose to reveal on their profiles. This is surprising as we expected that general concern for Internet privacy and unwanted audiences would both predict the amount of information that an individual chooses to reveal. A possible explanation is that concern for unwanted audiences affects how people manage the visibility of their profiles, but not the information that they reveal on their profiles in general. Perhaps those individuals who show a greater concern for unwanted audiences will also attempt to manage their profile by making it less visible rather than revealing less information. This could be further tested in future research. The third factor associated with information revelation is profile visibility. The less an individual closed their profile to others, the more information they revealed. This suggests that individuals, who are generally concerned about their privacy and hence close their profile to only friends, will reveal less information than those who do not manage their profiles.

The results of the present study also suggest that students employ a variety of protection strategies in order to address their privacy concerns. The strategies used most often by students to protect themselves were the exclusion personal information from their profiles, the use of private email messages to communicate, and alteration of the default privacy settings. We found that the strategies employed were linked to specific privacy concerns. Students in the interview sample who expressed concerns related to expressive privacy [DeCew 1997; Goldie 2006] tended to manage their concerns by either untagging or removing photographs or by making use of the limited profile to restrict certain contacts or groups of contacts from viewing specific types of personal information. Students who expressed concerns related to informational privacy [Goldie 2006; Westin 1972] restricted access to their profile and withheld information that could be used to link them to a physical location. The data therefore suggest that each privacy protection strategy has unique characteristics and supports students' privacy objectives in different ways.

In our study, students do not perceive the use of fake or inaccurate information to be a useful protective measure. Interview data suggest that students consider the falsification of personal information to be impractical and confusing because their friends and peers would question the validity of the information disclosed. As other researchers have noted, the public display of one's connections serves as verification on the reliability of identity claims ensuring that information on profiles is accurate and/or playful and ironic, rather than intentionally deceitful [Donth and boyd 2004; Lampe, Steinfield and Ellison 2007; see also Donath 2007 on signaling theory]. In this way, the structure of Facebook—that is, the fact that one's connections are linked to one's profile—encourages students to reveal information that is truthful rather than deceiving.

We conclude that examining privacy on Facebook requires the consideration of multiple factors. First, information revelation itself can consist of different types of elements. We identified both expressive and informational privacy as distinct dimensions that are managed differently by users [DeCew 1997; Goldie 2006]. Second, differences in findings across studies are difficult to explain because they may be the result of changes happening to the audience in Facebook or to the features available on the site. As Tufekci [2008] has suggested, by allowing the general public to use Facebook, students' perceptions of the site as a secure and private community may have been altered, affecting their behavior and information revelation practices. In this way, many students may be more likely to withhold certain types of information from their profiles than they were before general audiences could join Facebook.

The present study has a number of limitations. First, the findings are based on a small and non-representative sample. Second, the information revelation scale is based on a limited number of items. Third, the model needs to include further variables, for example control variables, such as age, gender, and area of study. Fourth, the results of the study can only be generalized to university students. Future research could seek to expand the present study by examining other user groups, such as high school or elementary school students, to see if their information revelation and privacy protection practices and behaviors on Facebook differ from those of university students.

7. Acknowledgements

The research was supported by a Social Sciences and Humanities Research Council of Canada Grant. This paper has tremendously benefitted from the help of Jacquie Burkell. We would like also to thank four anonymous reviewers for their insightful comments.

8. REFERENCES

[1] Acquisti, A. and Gross, R. 2006. Imagined communities: awareness, information sharing and privacy protection on the Facebook. In Proceedings of the 6th Workshop on Privacy Enhancing Technologies (Cambridge, UK, 2006).

[2] Barnes, S.B. 2006. A privacy paradox: social networking in the United States. First Monday. 11, 9 (September 2006) DOI=http://www.firstmonday.org/issues/issue11_9/barnes/index.html

[3] boyd, d. and Heer, J. 2006. Profiles as conversations: networked identity on Friendster. In Proceedings of the Hawaii International Conference on System Sciences (HICSS-39), Persistent Conversation Track (Kauai, Hawaii, January 4-7, 2006).

[4] boyd, d. 2008. Why youth (heart) social network sites: The role of networked publics in teenage social life. In Youth, Identity, and Digital Medias, Ed. D. Buckingham. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning, MIT Press, Cambridge, MA, 119-142.

[5] DeCew, J. W. 1997. In pursuit of privacy: Law, ethics & the rise of technology. Cornell University Press, Ithaca, NY.

[6] Donath, J. 2007. Signals in social supernets. Journal of Comupter-Mediated Communication. 13, 1 (2007), article 12. DOI: http://jcmc.indiana.edu/vol13/issue1/donath.html

[7] Donath, J. and d. boyd. 2004. Public displays of connection. BT Technology Journal 22, 4 (2004), 71-82.

[8] Fox, S., Rainie, L., Horrigan, J., Lenhart, A, Spooner, T., and Carter, C. 2000. Trust and privacy online: Why Americans want to rewrite the rules. PEW Internet and American Life Project (August 20, 2000). DOI= http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf

[9] Goffman, E. 1959. The presentation of self in everyday life. Doubleday Anchor, Garden City, NY.

[10] Goldie, J. L. 2006. Virtual communities and the social dimension of privacy. University of Ottawa Technology and Law Journal 3, 1 (2006), 133-167.

[11] Govani, T. and Pashley, H. 2005. Student awareness of the privacy implications when using Facebook. Paper presented at the Privacy Poster Fair at Carnegie Mellon University School of Library and Information Science (December 14, 2005). DOI=http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

[12] Gross, R. and Acquiti, A. 2005. Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on privacy in the electronic society (Alexandria, VA, November 7, 2005). ACM Press, New York.

[13] Joinson, A.N., Reips, U-D., Buchanan, T.B., and Paine Schofield, C.B. in press. Privacy, trust and self-disclosure online. Human-Computer Interaction. DOI= http://www.joinson.com/

[14] Jones, H. and Soltren, J.H. 2005. Facebook: Threats to privacy. Student Paper. DOI= http://www.swiss.ai.mit.edu/6095/student-papers/fall05-papers/facebook.pdf

[15] Lampe, C., Ellison, N., and Steinfield, C. 2006. A Face(book) in the crowd: Social searching vs. social browsing. In Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work (Banff, Alberta, Canada). ACM Press, 167-170.

[16] Lampe, C., Ellison, N., and Steinfield, C. 2007. A familiar Face(book): Profile elements as signals in an online social network. In Proceedings of the SIGHI conference on Human Factors in Computing Systems (San Jose, California, April 28-May 3, 2007). ACM Press, 435-444.

[17] Marx, G.T. n.d. Privacy and Technology (Revision of material that appeared in The World and I, September 1990 and Telekronik, January 1996). DOI=http://web.mit.edu/gtmarx/www/privantt.html

[18] Ritchie, J., Spencer, L., and O'Conner, W. 2003. Carrying out qualitative analysis. In Qualitative Research Practice: A guide for social science students and researchers, Eds. J. Rainie and J. Lewis. Sage Publications, Thousand Oaks, CA, 219-262.

[19] Sundén, J. 2003. Material Virtualities: Approaching online textual embodiment. Peter Lang, New York.

[20] Tufekci, Z. 2008. Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology and Society. 28, 20 (2008), 20-36.

[21] Viseu, A., Clement, A., and Aspinall, J. 2004. Situating privacy online: Complex perception and everyday practices. Information, Communication & Society. 7, 1 (2004), 92-114.

[22] Westin, A. F. 1972. Freedom and privacy. Atheneum. New York, NY.